Erdos distinct distances problem and extensions over finite spaces

THÈSE N^{O} 7787 (2017)

PRÉSENTÉE LE 12 JUIN 2017

À LA FACULTÉ DES SCIENCES DE BASE
CHAIRE DE GÉOMÉTRIE COMBINATOIRE
PROGRAMME DOCTORAL EN MATHÉMATIQUES

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

POUR L'OBTENTION DU GRADE DE DOCTEUR ÈS SCIENCES

PAR

Van Thang PHAM

acceptée sur proposition du jury:

Prof. F. Eisenbrand, président du jury
Prof. J. Pach, directeur de thèse
Prof. G. Tardos , rapporteur
Prof. A. V. Le, rapporteur
Prof. A. Shokrollahi, rapporteur

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE
Suisse
2017

To my parents

Acknowledgements

I will start by expressing my deepest gratitude and appreciation towards my supervisor Prof. János Pach for his invaluable support and non-stop encouragement. During my Phd time, what I have learned from János go much beyond Mathematics. He has taught me how to be patient and how to do math in an enjoyable way. Words are not enough to express all my gratitude to Prof. János Pach.

I would like to thank Prof. Gábor Tardos, Prof. Le Anh Vinh, Prof. Doowon Koh, Dr. Frank de Zeeuw, my co-authors, and all DCG, DISOPT members for many helpful and thorough discussions about various topics. I would like to express my sincere thanks to the jury members Prof. Friedrich Eisenbrand and Prof. Amin Shokrollahi.

Un grand "Merci" for Jocelyne, who has helped me so many times since my arrival in Lausanne. I am very lucky to have had (and still have) friends that made my stay in Lausanne memorable. Thank you Claudiu Valculescu, Tran The Dung, Hossein Nassajian Mojarrad, Hoang Duc Trung.

I also take this opportunity to thank the Mathematics Doctoral School at EPFL and the Swiss National Science Foundation for their support during my four years as a graduate student.

Above all, I thank my parents for their unconditional support. This thesis is devoted to them.

Lausanne, 04 May 2017 Pham Van Thang.

Abstract

In this thesis we study a number of problems in Discrete Combinatorial Geometry in finite spaces. The contents in this thesis are structured as follows:

1. In Chapter 1 we will state the main results and the notations which will be used throughout the thesis.

2. Chapter 2 is a version of the paper entitled "Sumsets of the distance sets in finite spaces", which has been submitted for publication, (2017).

3. Chapter 3 is a version of the paper entitled "Three-variable expanding polynomials and higher-dimensional distinct distances", which has been submitted for publication, co-authored with L. A. Vinh and de Zeeuw. The author was one of the main investigators of this chapter.

4. Chapter 4 is a postprint version of the paper entitled "Distinct distances on regular varieties over finite fields", Journal of Number Theory, **173** (2017), 602–613, co-authored with D. D. Hieu. The author was one of the main investigators of this chapter.

5. Chapter 5 is a postprint version of the paper entitled " Incidences between points and generalized spheres over finite fields and related problems", Forum Mathematicum, Volume 29, Issue 2 (Mar 2017), co-authored with N. D. Phuong and L. A. Vinh. The author was one of the main investigators of this chapter.

6. Chapter 6 is a version of the paper entitled "Distinct spreads in finite spaces", which has been submitted for publication, co-authored with B. Lund and L. A. Vinh. The author was one of the main investigators of this chapter.

7. Chapter 7 is a version of the paper entitled "Paths in pseudo-random graphs", which has been submitted for publication, co-authored with L. A. Vinh. The author was one of the main investigators of this chapter.

8. Chapter 8 is a version of the paper entitled "Conditional expanding bounds for two-variable functions over arbitrary fields", which has been submitted for

publication, co-authored with Hossein Nassajian Mojarrad. The author was one of the main investigators of this chapter.

9. Chapter 9 is a postprint version of the paper entitled "A Szemerédi-Trotter type theorem, sum-product estimates in finite quasifields, and related results", Journal of Combinatorial Theory Series A, **147** (2017), 55–74, co-authored with Michael Tait, Craig Timmons, Le Anh Vinh. The author was one of the main investigators of this chapter. The content of this chapter also appears in Michael Tait's Phd thesis.

10. In Chapter 10, we will mention some open problems on Erdős distinct distances problem and generalizations.

Key words: Finite fields, quasifields, incidence geometry, simplex, sumset, additive energy, spreads, angles, expanders, distinct distances, pseudo-random graphs, sum-product estimates.

Résumé

Dans cette thèse on étudie certains problèmes de géométrie discrète dans des espaces finis. Le contenu est structuré de la manière suivante :

1. Dans le premier chapitre on énonce les principaux résultats et les notations qu'on va utiliser au long de la thèse.

2. Le deuxième chapitre est une variante d'un article intitulé "Sumsets of the distance sets in finite spaces", qui a été soumis pour publication en 2017.

3. Le troisième chapitre est une variante d'un article intitulé "Three-variable expanding polynomials and higher-dimensional distinct distances", qui a été soumis pour publication, et qui a été coécrit avec L. A. Vinh et de Zeeuw. L'auteur a été l'un des Investigateurs Principaux.

4. Le quatrième chapitre est un post-print d'un article intitulé "Distinct distances on regular varieties over finite fields", publié dans le Journal of Number Theory, **173** (2017), 602–613., coécrit avec D. D. Hieu. L'auteur a été l'un des Investigateurs Principaux.

5. Le cinquième chapitre est une version postèrieure à l'impression d'un article intitulé " Incidences between points and generalized spheres over finite fields and related problems", Forum Mathematicum, Volume 29, Issue 2 (Mar 2017), coécrit avec N. D. Phuong et L. A. Vinh. L'auteur a été l'un des Investigateurs Principaux.

6. Le sixième chapitre est une version postèrieure à l'impression d'un article intitulé "Distinct spreads in finite spaces", qui a èté soumis pour publication et coécrit avec B. Lund et L. A. Vinh. L'auteur a été l'un des Investigateurs Principaux.

7. Le septième chapitre est une variante d'un article intitulé "Paths in pseudo-random graphs", soumis pour publication, et coécrit avec L. A. Vinh. L'auteur a été l'un des Investigateurs Principaux.

8. Le huitième chapitre est une variante d'un article intitulé "Conditional expanding bounds for two-variable functions over arbitrary fields", soumis pour publication, et coécrit avec Hossein Nassajian Mojarrad. L'auteur a été l'un des Investigateurs Principaux.

9. Le neuvième chapitre est une version postèrieure à l'impression d'un article intitulé "A Szemerédi-Trotter type theorem, sum-product estimates in finite quasifields, and related results", publié dans Journal of Combinatorial Theory Series A, **147** (2017), 55–74, coécrit avec Michael Tait, Craig Timmons, Le Anh Vinh. L'auteur a été l'un des Investigateurs Principaux. Le contenu de ce chapitre apparaît aussi dans la thèse de doctorat de Michael Tait.

10. Dans le dixième chapitre, on présente des problèmes ouvertes reliés au problème des distances distinctes d'Erdős, ainsi que des généralisations en ce sense.

Mots-clés : corps finis, quasifields, géometrie d'incidence, simplexe, sumset, énergie additive, spreads, angles, graphe expanseur, distances distinctes, graphes pseudo-aléatoires, estimations somme-produit.

Contents

1 Introduction

The classical Erdős distinct distances problem asks for the minimum number of distinct distances determined by a set of n points in the plane $\mathbb{R}^2$. In 1946, Erdős [25] showed that a $[\sqrt{n}] \times [\sqrt{n}]$ integer lattice generates $\Theta(n/\sqrt{\log n})$ distinct distances. From this construction, he conjectured that any set of n points in $\mathbb{R}^2$ spans at least $\Omega\left(n/\sqrt{\log n}\right)$ distinct distances. In 2010, this conjecture has been proved by Guth and Katz [29] using algebraic methods. They showed that a set of n points in $\mathbb{R}^2$ has at least $cn/\log n$ distinct distances for some positive constant c.

Let $\mathbb{F}_q$ be a finite field of order q, where q is an odd prime power. We denote the set of units in $\mathbb{F}_q$ by $\mathbb{F}_q^*$. For any two points $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^d$, we define the distance function between them as

$$||\mathbf{x}-\mathbf{y}|| := (x_1-y_1)^2+\cdots+(x_d-y_d)^2.$$

Although this distance function is not a metric in $\mathbb{F}_q^d$, it has some properties which are similar to the Euclidean distance function in $\mathbb{R}^d$ for example, it is preserved under orthogonal matrices and translations.

For a set $\mathscr{E} \subseteq \mathbb{F}_q^d$, we denote the set of distances determined by points in $\mathscr{E}$ by $\Delta(\mathscr{E})$. In 2004, Bourgain, Katz, and Tao [9] made the first investigation on the prime field analogue of the Erdős distinct distances problem. More precisely, they proved that for any set $\mathscr{E} \subseteq \mathbb{F}_p^2$ with $|\mathscr{E}| = p^\alpha$, $0 < \alpha < 2$, the distance set satisfies $|\Delta(\mathscr{E})| \geq |\mathscr{E}|^{\frac{1}{2}+\varepsilon}$ for some $\varepsilon > 0$ depending on α. In the case when $|\mathscr{E}| \ll p^{15/11}$, Stevens and de Zeeuw [76] improved this exponent to $|\mathscr{E}|^{8/15}$. This is the current best bound in the literature.

Here, and throughout the thesis, we use the following notations: $X \approx Y$ means that there exist positive absolute constants C_1 and C_2 which do not depend on X, Y, and q such that $C_1 Y < X < C_2 Y$; $X \ll Y$ means that there exists a positive absolute constant C that does not depend on X, Y and q such that $X \leq CY$; and $X = o(Y)$ means that

$X/Y \to 0$ as $q \to \infty$, where X, Y are viewed as functions in q.

For the case of large sets, the first explicit exponent for $|\Delta(\mathscr{E})|$ was given by Iosevich and Rudnev [44] in 2007 by using Fourier analytic methods. In particular, they proved that for $\mathscr{E} \subseteq \mathbb{F}_q^d$ with $|\mathscr{E}| \geq q^{\frac{d}{2}}$, the distance set satisfies $|\Delta(\mathscr{E})| \geq c \cdot \min\left\{q, |\mathscr{E}|/q^{(d-1)/2}\right\}$, for some positive constant c. This result leads to that if $|\mathscr{E}| \geq q^{(d+1)/2}$ then $|\Delta(\mathscr{E})| \geq cq$. Hart, Iosevich, Koh, Rudnev [35] indicated that the threshold $q^{\frac{d+1}{2}}$ can not be improved in odd dimensional spaces. There are several improvements on the exponent $(d+1)/2$ in even dimensional cases over recent years, for instance, see [6, 12, 32]. When $\mathscr{E}$ is a set in the unit sphere $S_1 \subset \mathbb{F}_q^d$, $d \geq 3$, i.e. the set of points $\mathbf{x} \in \mathbb{F}_q^d$ with $||\mathbf{x}|| = 1$, the authors of [35] showed that if $|\mathscr{E}| \gg q^{d/2}$ then $|\Delta(\mathscr{E})| \gg q$, but in odd dimensional cases, in order to get all distances, we still need the exponent $(d+1)/2$.

In this thesis, we consider variants of the Erdős distinct distances problem and related problems by using a wide range of mathematical tools and techniques including algebraic methods, spectral graph-theoretic techniques, and the probabilistic method. More precisely, we deal with the following problems: sumsets of the distance sets, three-variable expanding polynomials, distinct distances on regular varieties, point-sphere incidences, distinct spreads, paths in pseudo-random graphs, sum-product estimates over arbitrary fields, sum-product estimates over finite quasifields. For the sake of completeness, in each chapter, we give its own introduction and its relevant literature. The main purpose of this chapter is to briefly present the main results contained in this thesis, and the basic definitions required for each problem.

1.1 Main results

Sumsets of the distance sets

For a set $\mathscr{E} \subset \mathbb{F}_q^d$ and an integer $k \geq 1$, *the k-additive energy* of the distance set corresponding to $\mathscr{E}$, which is denoted by $E_+^k(\mathscr{E})$, is defined as the cardinality of

$$\left\{(\mathbf{x}_i, \mathbf{y}_i)_{i=1}^{2k} \in (\mathscr{E}^2)^{2k} \colon ||\mathbf{x}_1 - \mathbf{y}_1|| + \cdots + ||\mathbf{x}_k - \mathbf{y}_k|| = ||\mathbf{x}_{k+1} - \mathbf{y}_{k+1}|| + \cdots + ||\mathbf{x}_{2k} - \mathbf{y}_{2k}||\right\}.$$

In Chapter 2 we derive some improvements of results due to Shparlinski [71] as follows.

Theorem 1.1.1. *Let $\mathbb{F}_q$ be a finite field of order q with $q \equiv 3 \mod 4$. Let $k \geq 2$ be an integer, and $\mathscr{E}$ be a set in $\mathbb{F}_q^2$. Suppose that $|\mathscr{E}| \gg q$, then we have*

$$\left| E_+^k(\mathscr{E}) - \frac{|\mathscr{E}|^{4k}}{q} \right| \ll q^{2k-1} |\mathscr{E}|^{2k+\frac{1}{2}}.$$

Theorem 1.1.2. *Let $k \geq 2$ be an integer, and $\mathscr{E}$ be a set in $\mathbb{F}_q^d$, $d \geq 3$. We have the following*

$$\left| E_+^k(\mathscr{E}) - \frac{|\mathscr{E}|^{4k}}{q} \right| \ll q^{dk} |\mathscr{E}|^{2k}.$$

As consequences of Theorems 1.1.1 and 1.1.2, we obtain the following theorems on sumsets of the distance set.

Theorem 1.1.3. *Let $\mathbb{F}_q$ be a finite field of order q with $q \equiv 3 \mod 4$. Let $k \geq 2$ be an integer, and $\mathscr{E}$ be a set in $\mathbb{F}_q^2$. Suppose that $q^{1+\frac{1}{4k-1}} = o(|\mathscr{E}|)$, then we have*

$$|k\Delta(\mathscr{E})| = (1 - o(1))q.$$

Theorem 1.1.4. *Let $k \geq 2$ be an integer, and $\mathscr{E}$ be a set in $\mathbb{F}_q^d$ with $d \geq 3$. Suppose that $q^{\frac{d}{2}+\frac{1}{2k}} = o(|\mathscr{E}|)$, then we have*

$$|k\Delta(\mathscr{E})| = (1 - o(1))q.$$

Three-variable expanding polynomials

Let $\mathbb{F}$ be an arbitrary field. In this section, we use the convention that if $\mathbb{F}$ has positive characteristic, we denote the characteristic by p, while if $\mathbb{F}$ has characteristic zero, we set $p = \infty$. Thus, a condition like $N < p^{5/8}$ is restrictive in positive characteristic, but is vacuous in characteristic zero.

A polynomial $f \in \mathbb{F}[x_1, \ldots, x_k]$ is an *expander* if there are $\alpha > 1, \beta > 0$ such that for all sets $\mathscr{A}_1, \ldots, \mathscr{A}_k \subset \mathbb{F}$ of size $N \ll p^\beta$ we have

$$|f(\mathscr{A}_1 \times \cdots \times \mathscr{A}_k)| \gg N^\alpha.$$

In Chapter 3 we prove that any quadratic polynomial over arbitrary fields that is not of the form $g(h(x) + k(y) + l(z))$ is an expander. The precise statement is as follows.

Theorem 1.1.5. *Let $f \in \mathbb{F}[x, y, z]$ be a quadratic polynomial that depends on each variable and that does not have the form $g(h(x) + k(y) + l(z))$. Let $\mathscr{A}, \mathscr{B}, \mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}| = |\mathscr{B}| = |\mathscr{C}| = N$. Then*

$$|f(\mathscr{A} \times \mathscr{B} \times \mathscr{C})| \gg \min\left\{N^{3/2}, p\right\}.$$

Note that Theorem 1.1.5 can also viewed as Elekes-Rónyai's conjecture [24] for quadratic polynomials in three variables over arbitrary fields. As a consequence of Theorem

1.1.5, we obtain new bounds on Erdős distinct distances problem over arbitrary fields for Cartesian product structure sets.

Theorem 1.1.6. *For $\mathscr{A} \subset \mathbb{F}$ we have*

$$\left|\Delta(\mathscr{A}^d)\right| \gg \min\left\{|\mathscr{A}|^{2-\frac{1}{2^{d-1}}}, p\right\}.$$

In Chapter 3 we also derive some results on sum-product estimates which are improvements of Yazici et al.'s results [1].

Theorem 1.1.7. *For $\mathscr{A} \subset \mathbb{F}$ with $|\mathscr{A}| \ll p^{5/8}$ we have*

$$|\mathscr{A} + \mathscr{A}^2| \gg |\mathscr{A}|^{6/5}, \max\{|\mathscr{A} + \mathscr{A}|, |\mathscr{A}^2 + \mathscr{A}^2|\} \gg |\mathscr{A}|^{6/5}.$$

Distinct distances on regular varieties

Definition 1. *For $\mathscr{E} \subseteq \mathbb{F}_q^d$, let $\mathbf{1}_{\mathscr{E}}$ denote the characteristic function on $\mathscr{E}$. Let $F(\mathbf{x}) \in \mathbb{F}_q[x_1, \ldots, x_d]$ be a polynomial. The variety $\mathcal{V} := \{\mathbf{x} \in \mathbb{F}_q^d : F(\mathbf{x}) = 0\}$ is called a regular variety if $|\mathcal{V}| \approx q^{d-1}$ and $\widehat{\mathbf{1}_{\mathcal{V}}(\mathbf{m})} \ll q^{-(d+1)/2}$ for all $\mathbf{m} \in \mathbb{F}_q^d \setminus \mathbf{0}$, where*

$$\widehat{\mathbf{1}_{\mathcal{V}}(\mathbf{m})} = \frac{1}{q^d} \sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi(-\mathbf{m} \cdot \mathbf{x}) \mathbf{1}_{\mathcal{V}}(\mathbf{x}),$$

where χ is a non-trivial additive character of $\mathbb{F}_q$.

In Chapter 4 we prove some results on the number of distinct generalized distances in a set on a regular variety. These results are generalizations of recent results due to Covert, Koh, and Pi [19].

Theorem 1.1.8. *Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^d$. Suppose that $\mathcal{V} \subset \mathbb{F}_q^d$ is a regular variety, and assume that $k \geq 2$ is an integer and $\mathscr{E} \subseteq \mathcal{V}$. If $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathscr{E}|)$, then we have $\left\{Q(\mathbf{x}_1 + \cdots + \mathbf{x}_k) : \mathbf{x}_i \in \mathscr{E}, 1 \leq i \leq k\right\} \supseteq \mathbb{F}_q^*$.*

Theorem 1.1.9. *Let $P(\mathbf{x}) = \sum_{j=1}^{d} a_j x_j^{s_j} \in \mathbb{F}_q[x_1, \ldots, x_d]$ with $s_j \geq 2, \gcd(s_j, q) = 1$ and $a_j \neq 0$ for all $j = 1, \ldots, d$. Suppose that $\mathcal{V} \subset \mathbb{F}_q^d$ is a regular variety, and assume that $k \geq 2$ is an integer and $\mathscr{E} \subseteq \mathcal{V}$. If $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathscr{E}|)$, we have $|\{P(\mathbf{x}_1 + \cdots + \mathbf{x}_k) : \mathbf{x}_i \in \mathscr{E}, 1 \leq i \leq k\}| = (1 - o(1))q$.*

Point-sphere incidence bounds

Let $P = a_1 x_1^{c_1} + \cdots + a_d x_d^{c_d} \in \mathbb{F}_q[x_1, \ldots, x_d]$, where $2 \leq c_i \leq N$, for some constant $N > 0$, $\gcd(c_i, q) = 1$, and $a_i \in \mathbb{F}_q$ for all $1 \leq i \leq d$. We define the *generalized sphere*, or *P-sphere*, centered at $b = (b_1, \ldots, b_d)$ of radius $r \in \mathbb{F}_q$ to be the set $\{\mathbf{x} \in \mathbb{F}_q^d \mid P(\mathbf{x} - b) = r\}$.

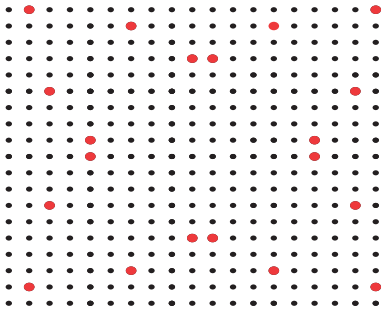

Figure 1.1 – The circle $x^2 + y^2 = 2$ in $\mathbb{F}_{19}^2$

Let $\mathscr{E}$ be a set of points in $\mathbb{F}_q^d$ and $\mathscr{S}$ be a set of P-spheres with arbitrary radii in $\mathbb{F}_q^d$. The number of incidences between $\mathscr{E}$ and $\mathscr{S}$, denoted by $I(\mathscr{E}, \mathscr{S})$, is the cardinality of $\{(p, s) \in \mathscr{E} \times \mathscr{S} : p \in s\}$.

In Chapter 5 we give the first result on the number of point-generalized sphere incidences in vector spaces over finite fields. Precisely, we prove the following theorem.

Theorem 1.1.10. *Let $\mathscr{E}$ be a set of points and $\mathscr{S}$ a set of P-spheres with arbitrary radii in $\mathbb{F}_q^d$. Then the number of incidences between points and spheres satisfies*

$$\left| I(\mathscr{E}, \mathscr{S}) - \frac{|\mathscr{E}||\mathscr{S}|}{q} \right| \leq q^{d/2} \sqrt{|\mathscr{E}||\mathscr{S}|}.$$

Given $\mathbf{x} \in \mathbb{F}_q^d$, we denote the pinned P-distance set determined by $\mathscr{E}$ and $\mathbf{x}$ by

$$\Delta_P(\mathscr{E}, \mathbf{x}) := \{P(\mathbf{y} - \mathbf{x}) \in \mathbb{F}_q \mid \mathbf{y} \in \mathscr{E}\}.$$

As an application of Theorem 1.1.10, we obtain the following result on the number of distinct pinned generalized distances.

Theorem 1.1.11. *Let $\mathscr{E} \subset \mathbb{F}_q^d$ with $|\mathscr{E}| > \sqrt{(1 - c^2)/c^4} \cdot q^{(d+1)/2}$ for some $0 < c < 1$. Then the number of points $p \in \mathscr{E}$ satisfying $|\Delta_P(\mathscr{E}, p)| > (1 - c)q$ is at least $(1 - c)|\mathscr{E}|$.*

Distinct spreads

For three points $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}_q^d$, the spread between two vectors $\overrightarrow{\mathbf{ab}}$ and $\overrightarrow{\mathbf{ac}}$ in $\mathbb{F}_q^d$, which is denoted by $S(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}})$ (or $S(\mathbf{b}, \mathbf{a}, \mathbf{c})$ for simplicity), is defined as

$$S\left(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}}\right) := 1 - \frac{\left(\overrightarrow{\mathbf{ab}} \cdot \overrightarrow{\mathbf{ac}}\right)^2}{\|\overrightarrow{\mathbf{ab}}\| \cdot \|\overrightarrow{\mathbf{ac}}\|},$$

where $\|\overrightarrow{\mathbf{x}}\| = x_1^2 + \cdots + x_d^2$. If either term in the denominator is 0, then $S(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}})$ is undefined.

It is clear that this definition is consistent with the square of the sine of the angle between two vectors $\overrightarrow{\mathbf{ab}}$ and $\overrightarrow{\mathbf{ac}}$ in Euclidean space

$$\sin(\theta)^2 = 1 - \frac{\left(\overrightarrow{\mathbf{ab}} \cdot \overrightarrow{\mathbf{ac}}\right)^2}{\|\overrightarrow{\mathbf{ab}}\| \cdot \|\overrightarrow{\mathbf{ac}}\|}.$$

In Chapter 6 we prove the following results on the number of distinct spreads generated by a point set in $\mathbb{F}_q^d$. These results can be viewed as applications of incidence bounds and distance results.

Theorem 1.1.12. *For any $\varepsilon > 0$, there exists $c > 0$ such that the following holds. Let $\mathcal{E}$ be a set of points in $\mathbb{F}_q^d$ with $d \geq 2$ even. If $|\mathcal{E}| \geq (1+\varepsilon)q^{d/2}$, then the number of distinct spreads determined by $\mathcal{E}$ is at least cq.*

Theorem 1.1.13. *For any $\varepsilon > 0$, there exists $c > 0$ such that the following holds. Let $\mathcal{E}$ be a set of points in $\mathbb{F}_q^d$ with $d \geq 3$ odd. If $|\mathcal{E}| \geq (1+\varepsilon)q^{(d+1)/2}$, then the number of distinct spreads determined by $\mathcal{E}$ is at least cq.*

In Chapter 6 we also show that the conditions on the size of $\mathcal{E}$ in Theorem 1.1.12 and Theorem 1.1.13 are sharp.

Paths in pseudo-random graphs

For a graph G, suppose that $\gamma_1 \geq \gamma_2 \geq \ldots \geq \gamma_n$ are the eigenvalues of its adjacency matrix. The second eigenvalue of G is defined as $\gamma(G) := \max\{\gamma_2, -\gamma_n\}$.

A graph $G = (V, E)$ is called an (n, d, γ)*-graph* if it is d-regular, has n vertices, and the second eigenvalue of G is at most γ. It is well known that G has certain random-like properties when γ is much smaller than the degree d. Noga Alon [49] established that

the number of copies of any fixed graph in every large subset of vertices in (n,d,γ)-graphs is close to the expected value.

Theorem 1.1.14 (**Alon**, Theorem 4.10 [49])**.** *Let H be a fixed graph with r edges, s vertices, and maximum degree Δ, and let $G=(V,E)$ be an (n,d,γ)-graph where $d \le 0.9n$. Let $m < n$ satisfy $\gamma(n/d)^{\Delta} = o(m)$. Then, for every subset $U \subset V$ of cardinality m, the number of (not necessarily induced) copies of H in U is*

$$(1+o(1))\frac{|U|^s}{|\mathtt{Aut}(H)|}\left(\frac{d}{n}\right)^r.$$

In Chapter 7 we give an asymptotically tight condition on the size of $U \subset V$ such that the number of paths of length k in U is close to the expected number for arbitrary $k \ge 1$. Our main results are as follows.

Theorem 1.1.15. *Let $G=(V,E)$ be an (n,d,γ)-graph. Suppose that $U \subseteq V$ with $\gamma\left(\frac{n}{d}\right) = o(|U|)$. For an integer $k \ge 1$, let $P_k(U)$ be the number of paths of length k in U, i. e.*

$$P_k(U) = \#\left\{(u_1,\dots,u_{k+1}) \in U^{k+1} \colon\ u_i u_{i+1} \in E(G), 1 \le i \le k\right\}.$$

Then we have

$$P_k(U) = (1+o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k.$$

Theorem 1.1.16. *Let $G=(V,E)$ be an (n,d,γ) graph. Suppose that $U \subseteq V$ with $\gamma\left(\frac{n}{d}\right) = o(|U|)$ and $k\left(\frac{n}{d}\right) = o(|U|)$. For an integer $k \ge 1$, let $D_k(U)$ be the number of paths of length k in U with distinct vertices, i.e.*

$$D_k(U) = \#\left\{(u_1,\dots,u_{k+1}) \in U^{k+1} \colon\ u_i u_{i+1} \in E(G), 1 \le i \le k,\ u_i \ne u_j, \forall\, i \ne j\right\}.$$

Then we have

$$D_k(U) = (1-o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k.$$

As applications, we obtain generalizations of the Erdős distinct distances problem in $\mathbb{F}_q^d$, which are improvements of results due to Bennett, Chapman, Covert, Hart, Iosevich, and Pakianathan [5].

Theorem 1.1.17. *Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^d$. Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d$, $d \ge 2$, and $k \ge 1$ be an integer. Let $t=(t_1,\dots,t_k) \in \mathbb{F}_q^t$ with $t_i \ne 0$, $1 \le i \le k$, we define*

$$P_k^t(\mathscr{E}) := |\{(p_1,\dots,p_{k+1}) \in \mathscr{E}\times\cdots\times\mathscr{E} : Q(p_i - p_{i+1}) = t_i,\ 1 \le i \le k\}|.$$

Suppose that $q^{\frac{d+1}{2}} = o(|\mathscr{E}|)$*, then we have*

$$P_k^t(\mathscr{E}) = (1+o(1))\frac{|\mathscr{E}|^{k+1}}{q^k}.$$

Theorem 1.1.18. *Let* Q *be a non-degenerate quadratic form on* $\mathbb{F}_q^d$*. Let* $\mathscr{E}$ *be a set in* $\mathbb{F}_q^d, d \geq 2$*, and* $k \geq 1$ *be an integer. Let* $t = (t_1, \ldots, t_k) \in \mathbb{F}_q^t$ *with* $t_i \neq 0, 1 \leq i \leq k$*, we define*

$$D_k^t(\mathscr{E}) := |\{(p_1, \ldots, p_{k+1}) \in \mathscr{E} \times \cdots \times \mathscr{E} : Q(p_i - p_{i+1}) = t_i,\ 1 \leq i \leq k, p_i \neq p_j, \forall\, i \neq j\}|.$$

Suppose that $kq = o(|\mathscr{E}|)$ *and* $q^{\frac{d+1}{2}} = o(|\mathscr{E}|)$*, then we have*

$$D_k^t(\mathscr{E}) = (1+o(1))\frac{|\mathscr{E}|^{k+1}}{q^k}.$$

Sum-product estimates over arbitrary fields

Let $\mathbb{F}$ be an arbitrary field. In this section, we use the convention that if $\mathbb{F}$ has positive characteristic, we denote the characteristic by p, while if $\mathbb{F}$ has characteristic zero, we set $p = \infty$. Thus, a condition like $N < p^{5/8}$ is restrictive in positive characteristic, but is vacuous in characteristic zero. We denote the set of non-zero elements in $\mathbb{F}$ by $\mathbb{F}^*$.

Let G be a subgroup of $\mathbb{F}^*$, and $g\colon G \to \mathbb{F}^*$ be an arbitrary function. We define

$$\mu(g) := \max_{t \in \mathbb{F}^*} \big|\{x \in G\colon\ g(x) = t\}\big|.$$

For $\mathscr{A}, \mathscr{B} \subset \mathbb{F}_p$ and two-variable functions $f(x,y)$ and $g(x,y)$ in $\mathbb{F}_p[x,y]$, Hegyvári and Hennecart [39], using graph theoretic techniques, proved that if $|\mathscr{A}| = |\mathscr{B}| = p^\alpha$, then

$$\max\big\{|f(\mathscr{A},\mathscr{B})|, |g(\mathscr{A},\mathscr{B})|\big\} \gg |\mathscr{A}|^{1+\Delta(\alpha)},$$

for some $\Delta(\alpha) > 0$. More precisely, they established the following results.

Theorem 1.1.19 (**Hegyvári and Hennecart**, [39])**.** *Let* G *be a subgroup of* $\mathbb{F}_p^*$*. Consider the function* $f(x,y) = g(x)(h(x)+y)$ *on* $G \times \mathbb{F}_p^*$*, where* $g, h\colon G \to \mathbb{F}_p^*$ *are arbitrary functions. Define* $m := \mu(g \cdot h)$*. For any subsets* $\mathscr{A} \subset G$ *and* $\mathscr{B}, \mathscr{C} \subset \mathbb{F}_p^*$*, we have*

$$\big|f(\mathscr{A},\mathscr{B})\big|\,|\mathscr{B}\cdot\mathscr{C}| \gg \min\left\{\frac{|\mathscr{A}||\mathscr{B}|^2|\mathscr{C}|}{pm^2}, \frac{p|\mathscr{B}|}{m}\right\}.$$

Theorem 1.1.20 (**Hegyvári and Hennecart**, [39])**.** *Let* G *be a subgroup of* $\mathbb{F}_p^*$*. Consider the function* $f(x,y) = g(x)(h(x)+y)$ *on* $G \times \mathbb{F}_p^*$*, where* $g, h\colon G \to \mathbb{F}_p^*$ *are arbitrary*

functions. Define $m := \mu(g)$. *For any subsets* $\mathscr{A} \subset G$, $\mathscr{B}, \mathscr{C} \subset \mathbb{F}_p^*$, *we have*

$$|f(\mathscr{A},\mathscr{B})||\mathscr{B}+\mathscr{C}| \gg \min\left\{\frac{|\mathscr{A}||\mathscr{B}|^2|\mathscr{C}|}{pm^2}, \frac{p|\mathscr{B}|}{m}\right\}.$$

Suppose $f(x,y) = g(x)(h(x)+y)$ with $\mu(g), \mu(h) = O(1)$ and $\mathscr{A} = \mathscr{B} = \mathscr{C}$. Then, it follows from Theorems 1.1.19 and 1.1.20 that

1. If $|\mathscr{A}| \gg p^{2/3}$, then we have

$$|f(\mathscr{A},\mathscr{A})||\mathscr{A}\cdot\mathscr{A}|, |f(\mathscr{A},\mathscr{A})||\mathscr{A}+\mathscr{A}| \gg p|\mathscr{A}|.$$

2. If $|\mathscr{A}| \ll p^{2/3}$, then we have

$$|f(\mathscr{A},\mathscr{A})||\mathscr{A}\cdot\mathscr{A}|, |f(\mathscr{A},\mathscr{A})||\mathscr{A}+\mathscr{A}| \gg |\mathscr{A}|^4/p. \tag{1.1.1}$$

In Chapter 8 we derive improvements and generalizations of Theorems 1.1.19 and 1.1.20 over arbitrary fields. Our first result is an improvement of Theorem 1.1.19.

Theorem 1.1.21. *Let* $f(x,y) = g(x)(h(x)+y)$ *be a function defined on* $\mathbb{F}^* \times \mathbb{F}^*$, *where* $g, h \colon \mathbb{F}^* \to \mathbb{F}^*$ *are arbitrary functions. Define* $m := \mu(g\cdot h)$. *For any subsets* $\mathscr{A}, \mathscr{B}, \mathscr{C} \subset \mathbb{F}^*$ *with* $|\mathscr{A}|, |\mathscr{B}|, |\mathscr{C}| \le p^{5/8}$, *we have*

$$\max\left\{|f(\mathscr{A},\mathscr{B})|, |\mathscr{B}\cdot\mathscr{C}|\right\} \gg \min\left\{\frac{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}}{m^{\frac{4}{5}}}, \frac{|\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}}{m^{\frac{2}{3}}}\right\}.$$

Corollary 1.1.22. *For* $\mathscr{A}, \mathscr{B}, \mathscr{C} \subset \mathbb{F}^*$ *with* $|\mathscr{A}|, |\mathscr{B}|, |\mathscr{C}| \le p^{5/8}$.

1. *Suppose that* $g(x) = 1$ *and* $h(x) = 1/x$, *then we have*

$$\max\left\{|\mathscr{A}^{-1}+\mathscr{B}|, |\mathscr{B}\cdot\mathscr{C}|\right\} \gg \min\left\{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}, |\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}, |\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}, |\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}\right\}.$$

2. *Suppose that* $g(x) = x$ *and* $h(x) = 1$, *then we have*

$$\max\left\{|\mathscr{A}(\mathscr{B}+1)|, |\mathscr{B}\cdot\mathscr{C}|\right\} \gg \min\left\{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}, |\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}, |\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}, |\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}\right\}.$$

This corollary is also an improvement of a recent result due to Zhelezov [96]. It follows from Corollary 1.1.22(2) that if $\mathscr{B} = \mathscr{A}$ and $\mathscr{C} = \mathscr{A}+1$ then we have $|\mathscr{A}(\mathscr{A}+1)| \gg |\mathscr{A}|^{6/5}$, which recovers the result of Stevens and de Zeeuw [76]. Our next result is the additive version of Theorem 1.1.21, which improves Theorem 1.1.20.

Theorem 1.1.23. *Let $f(x,y) = g(x)(h(x)+y)$ be a function defined on $\mathbb{F}^* \times \mathbb{F}^*$, where $g\colon \mathbb{F}^* \to \mathbb{F}^*$ are arbitrary functions. Define $m := \mu(g)$. For any subsets $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}^*$ with $|\mathscr{A}|,|\mathscr{B}|,|\mathscr{C}| \le p^{5/8}$, we have*

$$\max\{|f(\mathscr{A},\mathscr{B})|,|\mathscr{B}+\mathscr{C}|\} \gg \min\left\{\frac{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}}{m^{\frac{4}{5}}}, \frac{|\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}}{m^{\frac{2}{3}}}\right\}.$$

In the case $g(x) = x$ and $h(x) = 0$, we have the following result.

Corollary 1.1.24. *For $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}|,|\mathscr{B}|,|\mathscr{C}| \ll p^{5/8}$, we have*

$$\max\{|\mathscr{A}\cdot\mathscr{B}|,|\mathscr{B}+\mathscr{C}|\} \gg \min\left\{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}, |\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}, |\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}, |\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}\right\}.$$

When $\mathscr{A} = \mathscr{B} = \mathscr{C}$, we recover a result of Roche-Newton, Rudnev, and Shkredov [64], which states that $\max\{|\mathscr{A}+\mathscr{A}|,|\mathscr{A}\cdot\mathscr{A}|\} \gg |\mathscr{A}|^{6/5}$.

Sum-product estimates over finite quasifields

A set L with a binary operation $\cdot$ is called a *loop* if

1. the equation $a\cdot x = b$ has a unique solution in x for every $a,b \in L$,
2. the equation $y\cdot a = b$ has a unique solution in y for every $a,b \in L$, and
3. there is an element $e \in L$ such that $e\cdot x = x\cdot e = x$ for all $x \in L$.

A *(left) quasifield* Q is a set with two binary operations $+$ and $\cdot$ such that $(Q,+)$ is a group with additive identity 0, $(Q^*,\cdot)$ is a loop where $Q^* = Q\backslash\{0\}$, and the following three conditions hold:

1. $a\cdot(b+c) = a\cdot b + a\cdot c$ for all $a,b,c \in Q$,
2. $0\cdot x = 0$ for all $x \in Q$, and
3. the equation $a\cdot x = b\cdot x + c$ has exactly one solution for every $a,b,c \in Q$ with $a \neq b$.

The *kernel* K of a quasifield Q is the set of all elements $k \in Q$ that satisfy

1. $(x+y)\cdot k = x\cdot k + y\cdot k$ for all $x,y \in Q$, and

2. $(x \cdot y) \cdot k = x \cdot (y \cdot k)$ for all $x, y \in Q$.

Note that $(K, +)$ is an abelian subgroup of $(Q, +)$ and $(K^*, \cdot)$ is a group.

Note that any finite field is a quasifield. There are many examples of quasifields which are not fields; see for example, Chapter 5 of [21] or Chapter 9 of [42]. Quasifields appear extensively in the theory of projective planes. We note that in particular, in a quasifield multiplication need not be commutative nor associative. Throughout the chapter we must be careful about which side multiplication takes place on, and be wary that multiplicative inverses need not exist on both sides. Nonassociativity of multiplication is a bigger problem. Previous research on sum-product estimates requires associativity of multiplication for tools such as Plünnecke's inequality (see for example, [79] for the most general known sum-product theorem, the proof of which uses associativity of multiplication throughout).

In Chapter 9 we prove sum-product estimates in the setting of finite quasifields. These estimates generalize results of Vinh [85], of Garaev [27], and of Vu [95]. We also generalize results of Gyarmati and Sárközy [30] on the solvability of the equations $a+b=cd$ and $ab+1=cd$ over a finite field. Other analogous results that are known to hold in finite fields are generalized to finite quasifields. The precise statements of our results are as follows.

Theorem 1.1.25. *Let Q be a finite quasifield with q elements and $\mathscr{A} \subset Q \backslash \{0\}$. There is a positive constant c such that the following hold.*

If $q^{1/2} \ll |\mathscr{A}| < q^{2/3}$, then

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq c\frac{|\mathscr{A}|^2}{q^{1/2}}.$$

If $q^{2/3} \leq |\mathscr{A}| \ll q$, then

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq c(q|\mathscr{A}|)^{1/2}.$$

Theorem 1.1.26. *If Q is a finite quasifield with q elements and $\mathscr{A} \subset Q$, then there is a positive constant c such that*

$$|\mathscr{A}\cdot(\mathscr{A}+\mathscr{A})| \geq c\min\left\{q, \frac{|\mathscr{A}|^3}{q}\right\}.$$

Further, if $|\mathscr{A}| \gg q^{2/3}$, then one may take $c = 1 + o(1)$.

Theorem 1.1.27. *Let Q be a finite quasifield with q elements. If $\mathscr{A},\mathscr{B},\mathscr{C} \subset Q$, then*

$$|\mathscr{A} + \mathscr{B}\cdot\mathscr{C}| \geq q - \frac{q^3}{|\mathscr{A}||\mathscr{B}||\mathscr{C}| + q^2}$$

Theorem 1.1.28. *Let Q be a finite quasifield with q elements and let $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D} \subset Q$. If $\gamma \in Q$ and $N_\gamma(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D})$ is the number of solutions to $a+b+\gamma = c\cdot d$ with $a \in \mathscr{A}$, $b \in \mathscr{B}$, $c \in \mathscr{C}$, and $d \in \mathscr{D}$, then*

$$\left| N_\gamma(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}) - \frac{(q+1)|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{q^2+q+1} \right| \leq q^{1/2}\sqrt{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}.$$

Theorem 1.1.29. *Let $d \geq 1$ be an integer. If Q is a finite quasifield with q elements and $\mathscr{A} \subset Q$ with $|\mathscr{A}| \geq 2q^{\frac{d+2}{2d+2}}$, then*

$$Q = \mathscr{A} + \mathscr{A} + \underbrace{\mathscr{A}\cdot\mathscr{A} + \cdots + \mathscr{A}\cdot\mathscr{A}}_{d \text{ terms}}.$$

For the sake of following the content in each chapter easily, we repeat the statements of Expander mixing lemmas and the (n,d,γ)-form of some graphs in several chapters.

2 Sumsets of the distance sets in finite spaces

2.1 Introduction

For $\mathscr{E},\mathscr{F}\subset\mathbb{F}_q^d$ and an integer $k\geq 1$, *the k-additive energy* of the distance set corresponding to $\mathscr{E}$ and $\mathscr{F}$, which is denoted by $E_+^k(\mathscr{E},\mathscr{F})$, is defined as the cardinality of

$$\Big\{(\mathbf{x}_i,\mathbf{y}_i)_{i=1}^{2k}\in(\mathscr{E}\times\mathscr{F})^{2k}\colon ||\mathbf{x}_1-\mathbf{y}_1||+\cdots+||\mathbf{x}_k-\mathbf{y}_k||=||\mathbf{x}_{k+1}-\mathbf{y}_{k+1}||+\cdots+||\mathbf{x}_{2k}-\mathbf{y}_{2k}||\Big\}.$$

When $\mathscr{E}=\mathscr{F}$, we will use the notation $E_+^k(\mathscr{E})$ instead of $E_+^k(\mathscr{E},\mathscr{F})$.

Recently Shparlinski [71] used character sum techniques to discover properties of $E_+^2(\mathscr{E},\mathscr{F})$. More precisely, he proved the following theorem.

Theorem 2.1.1 (**Shparlinski**, [71]). *For $\mathscr{E},\mathscr{F}\subseteq\mathbb{F}_q^d$, we have*

$$\left|E_+^2(\mathscr{E},\mathscr{F})-\frac{|\mathscr{E}|^4|\mathscr{F}|^4}{q}\right|\leq q^{d-1}|\mathscr{E}|^3|\mathscr{F}|^3+q^{\frac{3d}{2}}|\mathscr{E}|^3|\mathscr{F}|^2.$$

As a consequence of Theorem 2.1.1, the author of [71] obtained the following result on a sumset of the distance set.

Theorem 2.1.2 (**Shparlinski**, [71]). *For $\mathscr{E},\mathscr{F}\subseteq\mathbb{F}_q^d$, we have*

$$|\Delta(\mathscr{E},\mathscr{F})+\Delta(\mathscr{E},\mathscr{F})|\geq\frac{1}{3}\min\left\{q,\frac{|\mathscr{E}||\mathscr{F}|^2}{q^{3d/2}},\frac{|\mathscr{E}||\mathscr{F}|}{q^{d-1}}\right\},$$

where $\Delta(\mathscr{E},\mathscr{F})=\Big\{||\mathbf{x}-\mathbf{y}||\colon\mathbf{x}\in\mathscr{E},\mathbf{y}\in\mathscr{F}\Big\}$.

Corollary 2.1.3 (**Shparlinski**, [71]). *Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d$. Suppose that $q^{\frac{d}{2}+\frac{1}{3}}=o(|\mathscr{E}|)$,*

then we have

$$|\Delta(\mathscr{E})+\Delta(\mathscr{E})| = (1-o(1))q.$$

The main purpose of this chapter is to give improvements of Theorems 2.1.1 and 2.1.2 by using methods from spectral graph theory. For the sake of simplicity of this chapter, we will consider the case $\mathscr{E}=\mathscr{F}$. We will give some discussions at the end of Section 3 for the case $\mathscr{E}\neq\mathscr{F}$. Our first result is the following.

Theorem 2.1.4. *Let $\mathbb{F}_q$ be a finite field of order q with $q\equiv 3 \mod 4$. Let $k\geq 2$ be an integer, and $\mathscr{E}$ be a set in $\mathbb{F}_q^2$ with $|\mathscr{E}|\gg q$. We have*

$$\left|E_+^k(\mathscr{E})-\frac{|\mathscr{E}|^{4k}}{q}\right| \ll q^{2k-1}|\mathscr{E}|^{2k+\frac{1}{2}}.$$

Our next theorem is a result on sumsets of the distance set.

Theorem 2.1.5. *Let $\mathbb{F}_q$ be a finite field of order q with $q\equiv 3 \mod 4$. Let $k\geq 2$ be an integer, and $\mathscr{E}$ be a set in $\mathbb{F}_q^2$. Suppose that $q^{1+\frac{1}{4k-1}}=o(|\mathscr{E}|)$, then we have*

$$|k\Delta(\mathscr{E})| = (1-o(1))q.$$

As consequences of Theorem 2.1.4 and Theorem 2.1.5, we are able to improve Theorem 2.1.1 and Corollary 2.1.3 in the case $d=2$.

Corollary 2.1.6. *Let $\mathbb{F}_q$ be a finite field of order q with $q\equiv 3 \mod 4$. Let $\mathscr{E}$ be a set in $\mathbb{F}_q^2$. Suppose that $|\mathscr{E}|\gg q$, then we have*

$$\left|E_+^2(\mathscr{E})-\frac{|\mathscr{E}|^{8}}{q}\right| \ll q^{3}|\mathscr{E}|^{9/2}.$$

Corollary 2.1.7. *Let $\mathbb{F}_q$ be a finite field of order q with $q\equiv 3 \mod 4$. Let $\mathscr{E}$ be a set in $\mathbb{F}_q^2$. Suppose that $q^{8/7}=o(|\mathscr{E}|)$, then we have*

$$|\Delta(\mathscr{E})+\Delta(\mathscr{E})| = (1-o(1))q.$$

When $\mathscr{E}$ is a subset in $\mathbb{F}_q^d$ with $d\geq 3$, by using the same techniques, we obtain a similar result as follows.

Theorem 2.1.8. *Let $\mathbb{F}_q$ be a finite field of order q. Let $k\geq 2$ be an integer, and $\mathscr{E}$ be a set*

in $\mathbb{F}_q^d$, $d \geq 3$. *We have the following*

$$\left| E_+^k(\mathscr{E}) - \frac{|\mathscr{E}|^{4k}}{q} \right| \ll q^{dk} |\mathscr{E}|^{2k}.$$

As an application of Theorem 2.1.8, we are able to improve Corollary 2.1.3 in the case $d \geq 3$.

Theorem 2.1.9. *Let* $\mathbb{F}_q$ *be a finite field of order* q. *Let* $k \geq 2$ *be an integer, and* $\mathscr{E}$ *be a set in* $\mathbb{F}_q^d$ *with* $d \geq 3$. *Suppose that* $q^{\frac{d}{2}+\frac{1}{2k}} = o(|\mathscr{E}|)$, *then we have*

$$|k\Delta(\mathscr{E})| = (1 - o(1))q.$$

The rest of this chapter is organized as follows: in Section 2, we recall some graph-theoretic tools; proofs of Theorems 2.1.4, 2.1.5, 2.1.8, and 2.1.9 are given in Section 3.

2.2 Graph-theoretic tools

Let G be a graph with n vertices. Suppose that $\gamma_1 \geq \gamma_2 \geq \ldots \geq \gamma_n$ are the eigenvalues of its adjacency matrix. The second eigenvalue of G is defined as $\gamma(G) := \max\{\gamma_2, -\gamma_n\}$. We say that a graph $G = (V, E)$ is an (n, d, γ)-*graph* if it is d-regular, has n vertices, and $\gamma(G) \leq \gamma$.

Suppose that B and C are two multi-sets of vertices in an (n, d, γ)-graph. Let $m_X(x)$ denote the multiplicity of x in X, and $e_m(B, C)$ be the number of edges with multiplicity between B and C in G, by multiplicity we mean that if there is an edge between $b \in B$ and $c \in C$, then this edge will be counted $m_B(b) \cdot m_C(c)$ times in $e_m(B, C)$. Recently, Hanson et al. [32] gave the following estimate on $e_m(B, C)$ in an (n, d, γ)-graph.

Lemma 2.2.1 ([32])**.** *Let* $G = (V, E)$ *be an* (n, d, γ)*-graph. The number of edges between two multi-sets of vertices* B *and* C *in* G *satisfies:*

$$\left| e_m(B, C) - \frac{d\left(\sum_{b\in B} m_B(b)\right)\left(\sum_{c\in C} m_C(c)\right)}{n} \right| \leq \gamma \sqrt{\sum_{b\in B} m_B(b)^2} \sqrt{\sum_{c\in C} m_C(c)^2},$$

where $m_X(x)$ *is the multiplicity of* x *in* X.

Sum-product graphs: We now define the *sum-product graph*, which is denoted by $SP_{q,d}$, as follows. The vertex set of $SP_{q,d}$ is the set $\mathbb{F}_q^d \times \mathbb{F}_q$. There is an edge between

two vertices $U = (\mathbf{a}, b)$ and $V = (\mathbf{c}, d) \in V(SP_{q,d})$ if and only if $\mathbf{a} \cdot \mathbf{c} = b + d$. Vinh [93] proved the following lemma on the (n, d, γ) form of $SP_{q,d}$.

Lemma 2.2.2 (**Vinh**, [93]). *For any $d \geq 1$, the sum-product graph $SP_{q,d}$ is an*

$$(q^{d+1}, q^d, \sqrt{2q^d}) - \textit{graph.}$$

2.3 Proofs of the main theorems

For $\mathscr{E} \subseteq \mathbb{F}_q^d$ and $\lambda \in \mathbb{F}_q$, we define

$$\nu_{\mathscr{E}}(\lambda) := \Big|\big\{(\mathbf{x}, \mathbf{y}) \in \mathscr{E} \times \mathscr{E} : ||\mathbf{x} - \mathbf{y}|| = \lambda\big\}\Big|.$$

In order to prove Theorems 2.1.4–2.1.9, we need the following lemmas, where the first one follows from the proof of [45, Theorem 3.5].

Lemma 2.3.1 (**Koh-Sun**, [46]). *Let $\mathbb{F}_q$ be a finite field of order q with $q \equiv 3 \mod 4$. Let $\mathscr{E}$ be a set in $\mathbb{F}_q^2$ with $|\mathscr{E}| \gg q$. Then we have*

$$E_+^1(\mathscr{E}) = \sum_{\lambda \in \mathbb{F}_q} \nu_{\mathscr{E}}(\lambda)^2 \leq \frac{|\mathscr{E}|^4}{q} + (1 + \sqrt{3})q|\mathscr{E}|^{5/2}.$$

For higher dimensional cases, the authors of [45] also proved a similar result for both cases $q \equiv 3 \mod 4$ and $q \equiv 1 \mod 4$, which can be found in [45, Propositions 2.3, 2.6]

Lemma 2.3.2 (**Koh-Sun**, [46]). *Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d$ with $d \geq 3$. Then we have*

$$E_+^1(\mathscr{E}) = \sum_{\lambda \in \mathbb{F}_q} \nu_{\mathscr{E}}(\lambda)^2 \leq \frac{|\mathscr{E}|^4}{q} + q^d|\mathscr{E}|^2.$$

We will use the following lemma to prove Theorem 2.1.4 and Theorem 2.1.8.

Lemma 2.3.3. *Let $k \geq 2$ be an integer, and $\mathscr{E}$ be a set in $\mathbb{F}_q^d$. We have*

$$\left|E_+^k(\mathscr{E}) - \frac{|\mathscr{E}|^{4k}}{q}\right| \ll q^d|\mathscr{E}|^2 E_+^{k-1}(\mathscr{E}).$$

Proof. We first define two multi-sets of vertices in the sum-product graph $SP_{q,2d}$ as follows:

$$\mathscr{B} := \big\{\big(-2\mathbf{x}_1, -2\mathbf{x}_2, -||\mathbf{x}_1|| - ||\mathbf{x}_2|| - ||\mathbf{x}_3 - \mathbf{y}_3|| - \cdots - ||\mathbf{x}_k - \mathbf{y}_k|| + ||\mathbf{x}_{k+1} - \mathbf{y}_{k+1}||\big) : \mathbf{x}_i, \mathbf{y}_i \in \mathscr{E}\big\},$$

$$\mathscr{C} := \left\{\left(\mathbf{y}_1, \mathbf{y}_2, -||\mathbf{y}_1|| - ||\mathbf{y}_2|| + ||\mathbf{x}_{k+2} - \mathbf{y}_{k+2}|| + \cdots + ||\mathbf{x}_{2k} - \mathbf{y}_{2k}||\right) : \mathbf{x}_i, \mathbf{y}_i \in \mathscr{E}\right\}.$$

For $(\mathbf{x}_i, \mathbf{y}_i)_{i=1}^{2k} \in (\mathscr{E} \times \mathscr{E})^{2k}$, if we have

$$||\mathbf{x}_1 - \mathbf{y}_1|| + \cdots + ||\mathbf{x}_k - \mathbf{y}_k|| = ||\mathbf{x}_{k+1} - \mathbf{y}_{k+1}|| + \cdots + ||\mathbf{x}_{2k} - \mathbf{y}_{2k}||,$$

then there is an edge between

$$\left(-2\mathbf{x}_1, -2\mathbf{x}_2, -||\mathbf{x}_1|| - ||\mathbf{x}_2|| - ||\mathbf{x}_3 - \mathbf{y}_3|| - \cdots - ||\mathbf{x}_k - \mathbf{y}_k|| + ||\mathbf{x}_{k+1} - \mathbf{y}_{k+1}||\right) \in \mathscr{B}$$

and

$$\left(\mathbf{y}_1, \mathbf{y}_2, -||\mathbf{y}_1|| - ||\mathbf{y}_2|| + ||\mathbf{x}_{k+2} - \mathbf{y}_{k+2}|| + \cdots + ||\mathbf{x}_{2k} - \mathbf{y}_{2k}||\right) \in \mathscr{C}$$

in the sum-product graph $SP_{q,2d}$. Therefore $E_+^k(\mathscr{E})$ is equal to the number of edges between $\mathscr{B}$ and $\mathscr{C}$ in $SP_{q,2d}$. In order to apply Lemma 2.2.1, we need to estimate upper bounds of $\sum_{b\in\mathscr{B}} m_{\mathscr{B}}(b)^2$ and $\sum_{c\in\mathscr{C}} m_{\mathscr{C}}(c)^2$. One can check that

$$\sum_{b\in\mathscr{B}} m_{\mathscr{B}}(b)^2 \leq |\mathscr{E}|^2 E_+^{k-1}(\mathscr{E}),\ \sum_{c\in\mathscr{C}} m_{\mathscr{C}}(c)^2 \leq |\mathscr{E}|^2 E_+^{k-1}(\mathscr{E}),\ \text{and}\ |\mathscr{B}| = |\mathscr{C}| = |\mathscr{E}|^{2k}.$$

It follows from Lemmas 2.2.1 and 2.2.2 that the number of edges between $\mathscr{B}$ and $\mathscr{C}$ in the sum-product graph $SP_{q,2d}$ satisfies

$$\left|E_+^k(\mathscr{E}) - \frac{|\mathscr{E}|^{4k}}{q}\right| \ll q^d |\mathscr{E}|^2 E_+^{k-1}(\mathscr{E}),$$

which concludes the proof of the lemma. □

Proof of Theorem 2.1.4: The proof proceeds by induction on k. The base case $k = 2$ follows from Lemma 2.3.1 and Lemma 2.3.3 with $d = 2$. Suppose that the claim holds for $k - 1 \geq 2$, we show that it also holds for k. Indeed, it follows from Lemma 2.3.3 with $d = 2$ that

$$\left|E_+^k(\mathscr{E}) - \frac{|\mathscr{E}|^{4k}}{q}\right| \ll q^2 |\mathscr{E}|^2 E_+^{k-1}(\mathscr{E}). \tag{2.3.1}$$

By induction hypothesis, we have

$$E_+^{k-1}(\mathscr{E}) \ll \frac{|\mathscr{E}|^{4(k-1)}}{q} + q^{2(k-1)-1} |\mathscr{E}|^{2(k-1)+\frac{1}{2}}. \tag{2.3.2}$$

Putting (2.3.1) and (2.3.2) together gives us

$$\left| E_+^k(\mathscr{E}) - \frac{|\mathscr{E}|^{4k}}{q} \right| \ll q^{2k-1}|\mathscr{E}|^{2k+\frac{1}{2}},$$

which ends the proof of the theorem. □

Proof of Theorem 2.1.5: For each $\lambda \in \mathbb{F}_q$, let N_λ be the number of tuples $(\mathbf{x}_1, \mathbf{y}_1, \ldots, \mathbf{x}_k, \mathbf{y}_k)$ in $\mathscr{E}^{2k}$ satisfying $||\mathbf{x}_1 - \mathbf{y}_1|| + ||\mathbf{x}_2 - \mathbf{y}_2|| + \cdots + ||\mathbf{x}_k - \mathbf{y}_k|| = \lambda$. We have $\sum_{\lambda \in \mathbb{F}_q} N_\lambda = |\mathscr{E}|^{2k}$. It is easy to check that $\sum_{\lambda \in \mathbb{F}_q} N_\lambda^2 = E_+^k(\mathscr{E})$. By applying the Cauchy-Schwarz inequality, we obtain the following

$$\sum_{\lambda \in \mathbb{F}_q} N_\lambda \leq \sqrt{|k\Delta(\mathscr{E})|} \left(E_+^k(\mathscr{E}) \right)^{1/2}.$$

This implies that

$$|k\Delta(\mathscr{E})| \geq \frac{|\mathscr{E}|^{4k}}{E_+^k(\mathscr{E})}.$$

Thus the theorem follows immediately from Theorem 2.1.4. □

Proof of Theorem 2.1.8: The proof of Theorem 2.1.8 is as similar as that of Theorem 2.1.4 except that we use Lemma 2.3.2 instead of Lemma 2.3.1. □

Proof of Theorem 2.1.9: The proof of Theorem 2.1.9 is as similar as that of Theorem 2.1.5 except that we use Theorem 2.1.8 instead of Theorem 2.1.4. □

Remarks: We conclude this chapter with some discussions on $E_+^2(\mathscr{E}, \mathscr{F})$ for $\mathscr{E}, \mathscr{F} \subseteq \mathbb{F}_q^d$ satisfying $|\mathscr{E}| < |\mathscr{F}|$. The main steps in our approach are Lemma 2.3.3 and upper bounds of $E_+^1(\mathscr{E}, \mathscr{F})$. For two sets $\mathscr{E}$ and $\mathscr{F}$ in $\mathbb{F}_q^2$ with $q \equiv 3 \mod 4$, it has been shown in [45] that

$$E_+^1(\mathscr{E}, \mathscr{F}) \ll \frac{|\mathscr{E}|^2|\mathscr{F}|^2}{q} + q|\mathscr{E}|^{3/2}|\mathscr{F}| \text{ for } d = 2, \tag{2.3.3}$$

and

$$E_+^1(\mathscr{E}, \mathscr{F}) \ll \frac{|\mathscr{E}|^2|\mathscr{F}|^2}{q} + q^{\frac{d-1}{2}}|\mathscr{E}|^2|\mathscr{F}| \text{ for odd } d \geq 3. \tag{2.3.4}$$

For $\mathscr{E},\mathscr{F}\subseteq\mathbb{F}_q^d$, one can follow the proof of Lemma 2.3.3 to obtain the following

$$\left|E_+^k(\mathscr{E},\mathscr{F})-\frac{|\mathscr{E}|^{2k}|\mathscr{F}|^{2k}}{q}\right|\ll q^d|\mathscr{E}||\mathscr{F}|E_+^{k-1}(\mathscr{E},\mathscr{F}). \tag{2.3.5}$$

If we put (2.3.3), (2.3.4), and (2.3.5) together, then we have

$$\left|E_+^2(\mathscr{E},\mathscr{F})-\frac{|\mathscr{E}|^4|\mathscr{F}|^4}{q}\right|\le q|\mathscr{E}|^3|\mathscr{F}|^3+q^3|\mathscr{E}|^{\frac{5}{2}}|\mathscr{F}|^2 \text{ for } d=2,$$

$$\left|E_+^2(\mathscr{E},\mathscr{F})-\frac{|\mathscr{E}|^4|\mathscr{F}|^4}{q}\right|\le q^{d-1}|\mathscr{E}|^3|\mathscr{F}|^3+q^{\frac{3d-1}{2}}|\mathscr{E}|^3|\mathscr{F}|^2 \text{ for odd } d\ge 3.$$

These results are also improvements of Theorem 2.1.1.

3 Three-variable expanding polynomials

3.1 Introduction

Let $\mathbb{F}$ be an arbitrary field. We use the convention that if $\mathbb{F}$ has positive characteristic, we denote the characteristic by p, while if $\mathbb{F}$ has characteristic zero, we set $p = \infty$. Thus, a condition like $N < p^{5/8}$ is restrictive in positive characteristic, but vacuous in characteristic zero.

Our aim in this chapter is to study the expansion behavior of polynomials, i.e., to determine when the value set of a polynomial on any finite set is significantly larger than the input. We wish to classify the polynomials that have this expanding property, and then to quantify the expansion. The following definition captures this property.

Definition 2. *A polynomial $f \in \mathbb{F}[x_1, \dots, x_k]$ is an* expander *if there are $\alpha > 1, \beta > 0$ such that for all sets $\mathscr{A}_1, \dots, \mathscr{A}_k \subset \mathscr{F}$ of size $N \ll p^\beta$ we have*

$$|f(\mathscr{A}_1 \times \cdots \times \mathscr{A}_k)| \gg N^\alpha.$$

Note that other sources may have slightly different definitions of expanders, but the essence is usually the same. One distinctive aspect is that we allow the sets $\mathscr{A}_i$ to be distinct; if one requires them to be the same, one obtains a strictly larger class of polynomials. Also note that if $\mathscr{A}$ is a subfield of $\mathbb{F}$ of size N, then $|f(\mathscr{A} \times \cdots \times \mathscr{A})| = N$, so in positive characteristic we must have $\beta < 1$. In characteristic zero, β plays no role.

In the wake of a recent result of Rudnev [66] (see Theorem 8.2.1), based on work of Guth and Katz [29], several expansion bounds for polynomials over arbitrary fields have been improved. Barak, Impagliazzo, and Wigderson [3] had proved that $f = xy+z$ is an expander over any prime field $\mathbb{F}_p$, with an unspecified $\alpha > 1$. Roche-Newton, Rudnev, and Shkredov [64] used [66] to improve the exponent to $\alpha = 3/2$ with $\beta = 2/3$,

over any field $\mathbb{F}$. In other words, they proved

$$|\mathscr{A}\mathscr{B}+\mathscr{C}| \gg N^{3/2}$$

for $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathscr{F}$ with $|\mathscr{A}| = |\mathscr{B}| = |\mathscr{C}| = N \ll p^{2/3}$. Aksoy-Yazici et al. [1] proved the same for $f = x(y+z)$. There are similar results for expanders in more than three variables, but establishing two-variable expanders over finite fields seems to be considerably harder. Essentially the only known example is $f(x,y) = x^2 + xy$, which Bourgain [8] proved to be an expander; Hegyvári and Hennecart [38] generalized this to polynomials of the form $f(x) + x^k g(y)$ (with certain exceptions). Stevens and De Zeeuw [76] improved the exponent for $x^2 + xy$ to $\alpha = 5/4$ with $\beta = 2/3$, again using [66].

Over $\mathbb{R}$, expanders are better understood. Elekes and Rónyai [24] discovered that over $\mathbb{R}$ the two-variable expanders are exactly those polynomials $f(x,y) \in \mathbb{R}[x,y]$ that do not have the additive form $g(h(x)+k(y))$ or the multiplicative form $g(h(x)k(y))$. Raz, Sharir, and Solymosi [63] improved the exponent to $\alpha = 4/3$. For three-variable polynomials, Schwartz, Solymosi, and De Zeeuw [69] proved that the only non-expanders over $\mathbb{R}$ have the form $g(h(x)+k(y)+l(z))$ or $g(h(x)k(y)l(z))$, and Raz, Sharir, and De Zeeuw [62] proved a quantitative version with $\alpha = 3/2$.

It is natural to conjecture that the same classification of expanders holds over arbitrary fields. Bukh and Tsimerman [11] and Tao [80] proved results in this direction for two-variable polynomials on large subsets of finite fields, but in general the expander question remains open for two-variable polynomials. We use the result of Rudnev [66] to make a first step towards classifying three-variable expanders over arbitrary fields, by determining which *quadratic* polynomials are expanders. The expanders $xy+z$ and $x(y+z)$, mentioned above, are special cases. Note that for quadratic polynomials the exceptional form $g(h(x)k(y)l(z))$ does not occur (if the polynomial depends on each variable).

Theorem 3.1.1. *Let $f \in \mathbb{F}[x,y,z]$ be a quadratic polynomial that depends on each variable and that does not have the form $g(h(x)+k(y)+l(z))$. Let $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}| = |\mathscr{B}| = |\mathscr{C}| = N$. Then*

$$|f(\mathscr{A}\times\mathscr{B}\times\mathscr{C})| \gg \min\left\{N^{3/2}, p\right\}.$$

In terms of our definition, this theorem says that if a quadratic $f \in \mathbb{F}[x,y,z]$ does not have the multiplicative form $g(h(x)+k(y)+l(z))$, then it is an expander with $\alpha = 3/2$ and $\beta = 2/3$. The theorem also gives expansion for $2/3 < \beta < 1$, with α shrinking as β approaches 1.

Consequences. One new expander included in our theorem is $f(x,y,z) = (x-y)^2+z$; all our applications rely on this special case of our main theorem.

We will show that we can use this expander to obtain a new bound on the expression $|\mathscr{A}+\mathscr{A}^2|$. This expression was first considered by Elekes, Nathanson, and Ruzsa [23], who observed that it has an expansion-like property, even though $f(x,y) = x+y^2$ is not an expander in the definition above (one could call it a "weak expander"). They showed that $|\mathscr{A}+\mathscr{A}^2| \gg |\mathscr{A}|^{5/4}$ for $\mathscr{A} \subset \mathbb{R}$, and the exponent was improved by Li and Roche-Newton [52] to 24/19 (up to a logarithmic factor in the bound). For $\mathscr{A} \subset \mathscr{F}_p$, Hart, Li, and Shen [37] proved that $|\mathscr{A}+\mathscr{A}^2| \gg |\mathscr{A}|^{147/146}$ for $|\mathscr{A}| \ll p^{1/2}$, which was improved by Aksoy Yazici et al. [1] to $|\mathscr{A}+\mathscr{A}^2| \gg |\mathscr{A}|^{11/10}$ for $|\mathscr{A}| \ll p^{5/8}$. Here we improve this bound further.

Theorem 3.1.2. *For $\mathscr{A} \subset \mathbb{F}$ with $|\mathscr{A}| \ll p^{5/8}$ we have*

$$|\mathscr{A}+\mathscr{A}^2| \gg |\mathscr{A}|^{6/5}.$$

A closely related expression is $|\mathscr{A}^2+\mathscr{A}^2|$, for which there are expansion-like bounds that are conditional on $|\mathscr{A}+\mathscr{A}|$ being small. Over $\mathbb{R}$, [23] proved $\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}^2+\mathscr{A}^2|\} \gg |\mathscr{A}|^{5/4}$, and the exponent was improved to 24/19 in [52] (up to logarithms). Over $\mathscr{F}_p$, [11] proved a quantitatively weaker version, and [1] proved that $\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}^2+\mathscr{A}^2|\} \gg |\mathscr{A}|^{8/7}$ for $|\mathscr{A}| \ll p^{3/5}$. We improve this bound as well.

Theorem 3.1.3. *For $\mathscr{A} \subset \mathbb{F}$ with $|\mathscr{A}| \ll p^{5/8}$ we have*

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}^2+\mathscr{A}^2|\} \gg |\mathscr{A}|^{6/5}.$$

It is worth noting that the bounds in Theorems 3.1.2 and 3.1.3 are numerically the same as the best known bounds for $\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\}$ [64] and $|\mathscr{A}\cdot(\mathscr{A}+1)|$ [76]; in each case the lower bound is $|\mathscr{A}|^{6/5}$ under the condition $|\mathscr{A}| \ll p^{5/8}$.

Our expansion bound for $f(x,y,z) = (x-y)^2+z$ also allows us to give inductive proofs of expansion bounds for the algebraic distance function in any number of variables. This idea is due to Hieu and Vinh [41] and Vinh [89], who used it to prove expansion bounds on large subsets of finite fields. Given $P \subset \mathbb{F}^d$, we define its *distance set* by

$$\Delta(P) := \left\{ \sum_{i=1}^{d} (x_i - y_i)^2 : (x_1,\dots,x_d), (y_1,\dots,y_d) \in P \right\}$$

Obtaining good expansion bounds for this function in $\mathbb{R}^2$ is the well-known *distinct distances problem* of Erdős [25], which is a central question in combinatorial geometry.

Here we prove a general bound for the number of distinct distances determined by a higher-dimensional Cartesian product. Note that as d increases this bound converges to $|\mathscr{A}|^2$ (up to constants).

Theorem 3.1.4. *For $\mathscr{A} \subset \mathbb{F}$ we have*

$$\left|\Delta(\mathscr{A}^d)\right| \gg \min\left\{|\mathscr{A}|^{2-\frac{1}{2^{d-1}}}, p\right\}.$$

For $d = 2$ we recover the result of Petridis [60] that $|\Delta(\mathscr{A}^2)| \gg \min\{|\mathscr{A}|^{3/2}, p\}$, which is the current best bound for distinct distances on Cartesian products over general fields. For large subsets of prime fields, we recover a result of Hieu and Vinh [41].

Finally, we consider $\mathbb{F} = \mathbb{R}$, which is of course the field for which Erdős [25] introduced the distinct distances problem. He observed that for $\mathscr{A} = \{1, \dots, N\}$ we have $|\Delta(\mathscr{A}^2)| \ll |\mathscr{A}|^2/\sqrt{\log|\mathscr{A}|}$ and $|\Delta(\mathscr{A}^d)| \ll |\mathscr{A}|^2 = (|\mathscr{A}^d|)^{2/d}$ for $d \geq 3$. He later conjectured that these bounds are optimal for arbitrary point sets, i.e., that $|\Delta(P)| \gg |P|/\sqrt{\log|P|}$ for all $P \subset \mathbb{R}^2$, and $|\Delta(P)| \gg |P|^{2/d}$ for all $P \subset \mathbb{R}^d$ with $d \geq 3$. Guth and Katz [29] almost solved this for $d = 2$, by proving that

$$|\Delta(P)| \gg |P|/\log|P| \tag{3.1.1}$$

for any $P \subset \mathbb{R}^2$. For $d \geq 3$, the best lower bound is due to Solymosi and Vu [74]. It is roughly speaking of the form

$$|\Delta(P)| \gg |P|^{\frac{2}{d}-\frac{1}{d^2}};$$

see Sheffer [70] for the exact expression (incorporating [29]).

It follows from [29] that for any $\mathscr{A} \subset \mathbb{R}$ we have $|\Delta(\mathscr{A}^d)| \gg |\mathscr{A}|^2/\log|\mathscr{A}|$, since the set $(\mathscr{A}-\mathscr{A})^2 + (\mathscr{A}-\mathscr{A})^2$ is contained in any set of the form $(\mathscr{A}-\mathscr{A})^2 + \cdots + (\mathscr{A}-\mathscr{A})^2$. By taking the distinct distances bound of [29] as the base case for the inductive argument with $(x-y)^2 + z$ that we used to prove Theorem 3.1.4, we obtain an improvement on the exponent of the logarithm.

Theorem 3.1.5. *For $\mathscr{A} \subset \mathbb{R}$ and $d \geq 2$ we have*

$$\left|\Delta(\mathscr{A}^d)\right| \gg \frac{|\mathscr{A}|^2}{\log^{1/2^{d-2}}|\mathscr{A}|}.$$

We note that this theorem can also be proved without Rudnev's theorem [66], by using only the Szemerédi–Trotter theorem [77] and the Guth–Katz bound [29]; see Section 3.3.

3.2 Three-variable expanding polynomials

Our main tool is a point-plane incidence bound of Rudnev [66]. We use the following slightly strengthened version proved by De Zeeuw [20] (and our proof relies on this strengthening). We write $\mathscr{I}(\mathscr{R},\mathscr{S}) = |\{(r,s) \in \mathscr{R} \times \mathscr{S} : r \in s\}|$ for the number of *incidences* of $\mathscr{R}$ and $\mathscr{S}$.

Theorem 3.2.1 (Rudnev)**.** *Let $\mathscr{R}$ be a set of points in $\mathbb{F}^3$ and let $\mathscr{S}$ be a set of planes in $\mathbb{F}^3$, with $|\mathscr{R}| \ll |\mathscr{S}|$ and $|\mathscr{R}| \ll p^2$. Suppose that there is no line that contains k points of $\mathscr{R}$ and is contained in k planes of $\mathscr{S}$. Then*

$$\mathscr{I}(\mathscr{R},\mathscr{S}) \ll |\mathscr{R}|^{1/2}|\mathscr{S}| + k|\mathscr{S}|.$$

To prove Theorem 3.1.1, we divide the quadratic polynomials into two types: those with only one or two of the mixed terms xy, xz, yz, and those with all three. Our approach to both types is similar, but it appears technically simpler to treat these types separately.

Lemma 3.2.2. *Consider a polynomial*

$$f(x,y,z) = axy + bxz + r(x) + s(y) + t(z),$$

for polynomials $r,s,t \in \mathbb{F}[u]$ of degree at most two, with $a \neq 0$ and $t(z)$ not constant. Let $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}|,|\mathscr{B}| \leq |\mathscr{C}|$. Then

$$|f(\mathscr{A}\times\mathscr{B}\times\mathscr{C})| \gg \min\left\{|\mathscr{A}|^{1/2}|\mathscr{B}|^{1/2}|\mathscr{C}|^{1/2}, p\right\}.$$

Proof. We may assume $|\mathscr{A}||\mathscr{B}||\mathscr{C}| \ll p^2$. Otherwise, we can remove elements from the sets, while preserving $|\mathscr{A}|,|\mathscr{B}| \leq |\mathscr{C}|$, until we have sets $\mathscr{A}',\mathscr{B}',\mathscr{C}'$ that do satisfy $|\mathscr{A}'||\mathscr{B}'||\mathscr{C}'| \ll p^2$. The proof below then gives $|f(\mathscr{A}'\times\mathscr{B}'\times\mathscr{C}')| \gg |\mathscr{A}'|^{1/2}|\mathscr{B}'|^{1/2}|\mathscr{C}'|^{1/2} = p$.

We let E be the number of solutions $(x,y,z,x',y',z') \in (\mathscr{A}\times\mathscr{B}\times\mathscr{C})^2$ of

$$f(x,y,z) = f(x',y',z').$$

We can rewrite this equation to

$$ayx - ax'y' + (bxz + r(x) + t(z) - s(y')) = bx'z' + r(x') + t(z') - s(y).$$

We define a point set

$$\mathscr{R} := \{(x, y', bxz + r(x) + t(z) - s(y')) : (x, y', z) \in \mathscr{A} \times \mathscr{B} \times \mathscr{C}\}$$

and a plane set

$$\mathscr{S} = \{ayX - ax'Y + Z = bx'z' + r(x') + t(z') - s(y) : (x', y, z') \in \mathscr{A} \times \mathscr{B} \times \mathscr{C}\}.$$

A point in $\mathscr{R}$ corresponds to at most two points $(x, y', z) \in \mathscr{A} \times \mathscr{B} \times \mathscr{C}$, since x and y' are determined by the first two coordinates, and z is then determined with multiplicity at most two by the quadratic expression in the third coordinate. Here we use the assumption that $t(z)$ is not constant; the only exception occurs when $t(z)$ is linear and its main term is cancelled out by bxz; this is negligible since it only occurs for one value of x. The same argument shows that a plane in $\mathscr{S}$ corresponds to at most two points $(x', y, z') \in \mathscr{A} \times \mathscr{B} \times \mathscr{C}$. Thus we have $|\mathscr{R}|, |\mathscr{S}| \approx |\mathscr{A}||\mathscr{B}||\mathscr{C}|$.

A solution of $f(x, y, z) = f(x', y', z')$ corresponds to an incidence between a point in $\mathscr{R}$ and a plane in $\mathscr{S}$. Conversely, an incidence corresponds to at most four solutions, since the point and the plane have multiplicity at most two. Hence $\mathscr{I}(\mathscr{R}, \mathscr{S}) \approx E$. By assumption we have $|\mathscr{R}| \approx |\mathscr{A}||\mathscr{B}||\mathscr{C}| \ll p^2$, which allows us to apply Theorem 8.2.1. We need to prove an upper bound on the k such that there is a line containing k points of $\mathscr{R}$ and contained in k planes of $\mathscr{S}$.

The projection of $\mathscr{R}$ to the first two coordinates is $\mathscr{A} \times \mathscr{B}$, so a line contains at most $\max\{|\mathscr{A}|, |\mathscr{B}|\}$ points of $\mathscr{R}$, unless it is vertical, in which case it could contain $|\mathscr{C}|$ points of $\mathscr{R}$. However, the planes in $\mathscr{S}$ contain no vertical lines (since they are defined by equations in which the coefficient of Z is non-zero), so in this case the condition of Theorem 8.2.1 holds with $k = \max\{|\mathscr{A}|, |\mathscr{B}|\} \leq |\mathscr{A}|^{1/2}|\mathscr{B}|^{1/2}|\mathscr{C}|^{1/2}$.

Thus we get

$$E \approx \mathscr{I}(\mathscr{R}, \mathscr{S}) \ll |\mathscr{A}|^{3/2}|\mathscr{B}|^{3/2}|\mathscr{C}|^{3/2}.$$

By the Cauchy-Schwartz inequality we have $|\mathscr{A}|^2|\mathscr{B}|^2|\mathscr{C}|^2 \leq E \cdot |f(\mathscr{A} \times \mathscr{B} \times \mathscr{C})|$, so we get

$$|f(\mathscr{A} \times \mathscr{B} \times \mathscr{C})| \gg |\mathscr{A}|^{1/2}|\mathscr{B}|^{1/2}|\mathscr{C}|^{1/2}.$$

This finishes the proof. □

It would not be hard to generalize Lemma 3.2.2 to polynomials of the form

$$f(x, y, z) = g(x)h(y) + k(x)l(z) + r(x) + s(y) + t(z),$$

with the resulting bound depending on the degrees of g, h, k, l, r, s, t.

Lemma 3.2.3. *Let $f \in \mathbb{F}[x,y,z]$ be a polynomial of the form*

$$f(x,y,z) = axy + bxz + cyz + dx^2 + ey^2 + gz^2,$$

with none of a,b,c zero, and with $4eg \neq c^2$. Let $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}| = |\mathscr{B}| = |\mathscr{C}| = N$. Then

$$|f(\mathscr{A}\times\mathscr{B}\times\mathscr{C})| \gg \min\left\{N^{3/2}, p\right\}.$$

Proof. We may assume $|\mathscr{A}||\mathscr{B}||\mathscr{C}| \ll p^2$ as in the proof of Lemma 3.2.2. We again bound the number E of solutions $(x,y,z,x',y',z') \in (\mathscr{A}\times\mathscr{B}\times\mathscr{C})^2$ of $f(x,y,z) = f(x',y',z')$. We rewrite the equation to

$$(ay+bz)x - x'(ay'+bz') + (dx^2 - (e(y')^2 + cy'z' + g(z')^2) = d(x')^2 - (ey^2 + cyz + gz^2).$$

We define a point set

$$\mathscr{R} := \{(x, ay'+bz', dx^2 - (e(y')^2 + cy'z' + g(z')^2) : (x,y',z') \in \mathscr{A}\times\mathscr{B}\times\mathscr{C}\}$$

and a plane set

$$\mathscr{S} = \{(ay+bz)X - x'Y + Z = d(x')^2 - (ey^2 + cyz + gz^2) : (x',y,z) \in \mathscr{A}\times\mathscr{B}\times\mathscr{C}\}.$$

We show that a point $(u,v,w) \in \mathscr{R}$ corresponds to at most two points $(x,y',z') \in \mathscr{A}\times\mathscr{B}\times\mathscr{C}$. Suppose that we have $u = x, v = ay'+bz', w = dx^2 - e(y')^2 - cy'z' - g(z')^2$. Then

$$w = du^2 - e(y')^2 - cy'\frac{v-ay'}{b} - g\left(\frac{v-ay'}{b}\right)^2,$$

or equivalently

$$\left(b^2d - abc + a^2g\right)(y')^2 + \left(bcv - 2agv\right)y' + b^2w - b^2du^2 + gv^2 = 0.$$

We do not have both $b^2d - abc + a^2g = 0$ and $bc - 2ag = 0$, since these two equations would imply $4eg = c^2$, contradicting the assumption of the lemma. Hence there are at most two values of y' corresponding to (u,v,w), with unique corresponding x, z'.

The same argument shows that a plane in $\mathscr{S}$ corresponds to at most two points (x',y,z). Hence we have $|\mathscr{R}|, |\mathscr{S}| \approx |\mathscr{A}||\mathscr{B}||\mathscr{C}|$ and $\mathscr{I}(\mathscr{R},\mathscr{S}) \approx E$. By the assumption at the start of the proof we have $|\mathscr{R}| \approx |\mathscr{A}||\mathscr{B}||\mathscr{C}| \ll p^2$. This allows us to apply Theorem 8.2.1, if we find an upper bound on the maximum number of collinear points in $\mathscr{R}$.

The point set $\mathscr{R}$ is covered by $|\mathscr{A}|$ planes of the form $x = x_0$. If a line is not in one of these planes, then it intersects $\mathscr{R}$ in at most $|\mathscr{A}| = N$ points. Let ℓ be a line contained in a plane $x = x_0$. The points of $\mathscr{R}$ in this plane lie on a curve which is either a parabola or a line. In the first case, ℓ intersects the parabola in at most two points. In the second case, ℓ either intersects the line in one point, or it equals that line, which contains $|\mathscr{C}|$ points. It is easy to see from the equations that for distinct y' we get distinct curves, so the case where the curve equals ℓ occurs at most once. This implies that ℓ contains at most $2|\mathscr{B}| + |\mathscr{C}| \ll N$ points of $\mathscr{R}$.

With $k = N$ we get $E \approx \mathscr{I}(\mathscr{R}, \mathscr{S}) \ll (N^3)^{3/2} + N \cdot N^3 \ll N^{9/2}$, and again using Cauchy-Schwartz we get $|f(\mathscr{A} \times \mathscr{B} \times \mathscr{C})| \gg N^{3/2}$. This finishes the proof. □

We now combine the two lemmas to prove Theorem 3.1.1.

Proof of Theorem 3.1.1. Let $f(x, y, z)$ be a quadratic polynomial that is not of the form $g(h(x) + k(y) + l(z))$. In particular, f has at least one of the mixed terms xy, xz, yz, since otherwise it would be of the form $h(x) + k(y) + l(z)$. If one of the terms xy, xz, yz does not occur in f, then Lemma 3.2.2 proves the theorem.

Thus we can assume that f has the form

$$f(x, y, z) = axy + bxz + cyz + r(x) + s(y) + t(z),$$

with a, b, c non-zero and r, s, t polynomials of degree at most two. We may assume that r, s, t have no constant or linear terms. Indeed, any constant term can be removed immediately, and any linear terms can be removed by a change of variables of the form $\widetilde{x} = p_1 x + q_1, \widetilde{y} = p_2 y + q_2, \widetilde{z} = p_3 z + q_3$. Thus we assume that f has the form

$$f(x, y, z) = axy + bxz + cyz + dx^2 + ey^2 + gz^2.$$

The assumption that f is not of the form $g(h(x) + k(y) + l(z))$, which still holds after the linear change of variables, implies that the equations $4de = a^2, 4dg = b^2, 4eg = c^2$ do not all hold. Otherwise, we could write $f = (\sqrt{d}x + \sqrt{e}y + \sqrt{g}z)^2$ (if d, e, g are not squares in $\mathbb{F}$, we can write $f = (d\sqrt{eg}x + e\sqrt{dg}y + g\sqrt{de}z)^2/deg$). By permuting the variables, we can assume that $4eg \neq c^2$. Then we can apply Theorem 3.2.3, which finishes the proof. □

3.3 Consequences of Theorem 3.1.1

Proof of Theorem 3.1.2. We consider the equation

$$(x-y)^2+z=t. \tag{3.3.1}$$

Observe that for any $a,b,c\in\mathscr{A}$, a solution of (3.3.1) is given by $x=a+b^2\in\mathscr{A}+\mathscr{A}^2$, $y=b^2\in\mathscr{A}^2$, $z=c\in\mathscr{A}$, and $t=c+a^2\in\mathscr{A}+\mathscr{A}^2$. Thus we have

$$|\mathscr{A}|^3\le\left|\{(x,y,z,t)\in(\mathscr{A}+\mathscr{A}^2)\times\mathscr{A}^2\times\mathscr{A}\times(\mathscr{A}+\mathscr{A}^2):(x-y)^2+z=t\}\right|. \tag{3.3.2}$$

If we set

$$E=\left|\{(x,y,z,x',y',z')\in((\mathscr{A}+\mathscr{A}^2)\times\mathscr{A}^2\times\mathscr{A})^2:\,(x-y)^2+z=(x'-y')^2+z'\}\right|,$$

then (3.3.2) and the Cauchy-Schwarz inequality give

$$\frac{|\mathscr{A}|^6}{|\mathscr{A}+\mathscr{A}^2|}\le E. \tag{3.3.3}$$

We now partly follow the proof of Lemma 3.2.2 for $f(x,y,z)=(x-y)^2+z$. We define a point set

$$\mathscr{R}:=\{(x,y',x^2+z-(y')^2):(x,y',z)\in(\mathscr{A}+\mathscr{A}^2)\times\mathscr{A}^2\times\mathscr{A}\}$$

and a plane set

$$\mathscr{S}:=\{-2yX+2x'Y+Z=(x')^2+z'-y^2:(x',y,z')\in(\mathscr{A}+\mathscr{A}^2)\times\mathscr{A}^2\times\mathscr{A}\}.$$

We are already done if $|\mathscr{A}+\mathscr{A}^2|\gg|\mathscr{A}|^{6/5}$, so we can assume that $|\mathscr{A}+\mathscr{A}^2|\ll|\mathscr{A}|^{6/5}$, which gives $|\mathscr{R}|\approx|\mathscr{A}+\mathscr{A}^2||\mathscr{A}^2||\mathscr{A}|\ll|\mathscr{A}|^{16/5}\ll p^2$, using the assumption $|\mathscr{A}|\ll p^{5/8}$. Thus we can apply Theorem 8.2.1. By the same argument as in the proof of Lemma 3.2.2, we can use $k=\max\{|\mathscr{A}+\mathscr{A}^2|,|\mathscr{A}^2|\}=|\mathscr{A}+\mathscr{A}^2|$, so we get

$$E\ll|\mathscr{A}+\mathscr{A}^2|^{3/2}|\mathscr{A}|^3+|\mathscr{A}+\mathscr{A}^2|^2|\mathscr{A}|^2. \tag{3.3.4}$$

If the second term is larger than the first, then we have $|\mathscr{A}+\mathscr{A}^2|\gg|\mathscr{A}|^2$, and we would be done. Otherwise, the first term is larger, so combining (3.3.3) and (3.3.4) gives

$$\frac{|\mathscr{A}|^6}{|\mathscr{A}+\mathscr{A}^2|}\ll|\mathscr{A}+\mathscr{A}^2|^{3/2}|\mathscr{A}|^3,$$

which implies that

$$|\mathscr{A}+\mathscr{A}^2| \gg |\mathscr{A}|^{6/5}.$$

This completes the proof of the theorem. □

Proof of Theorem 3.1.3. The proof is very similar to that of Theorem 3.1.2, and we omit most of the details. The key observation, analogous to (3.3.2), is

$$|\mathscr{A}|^3 \leq \left|\left\{(x,y,z,t) \in (\mathscr{A}+\mathscr{A}) \times \mathscr{A} \times \mathscr{A}^2 \times (\mathscr{A}^2+\mathscr{A}^2) : (x-y)^2+z=t\right\}\right|.$$

By following the steps in the proof of Theorem 3.1.2 we now obtain

$$\frac{|\mathscr{A}|^6}{|\mathscr{A}^2+\mathscr{A}^2|} \ll |\mathscr{A}+\mathscr{A}|^{3/2}|\mathscr{A}|^3$$

under the condition $|\mathscr{A}| \ll p^{5/8}$, which gives

$$|\mathscr{A}+\mathscr{A}|^3|\mathscr{A}^2+\mathscr{A}^2|^2 \gg |\mathscr{A}|^6.$$

This proves the theorem. □

To prove (a generalization of) Theorem 3.1.4, we use a special case of Lemma 3.2.2.

Corollary 3.3.1. *Let $g \in \mathbb{F}[x,y]$ be a quadratic polynomial with a non-zero xy-term. Let $\mathscr{A},\mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}| \leq |\mathscr{C}|$. Then*

$$|g(\mathscr{A}\times\mathscr{A})+\mathscr{C}| \gg \min\left\{|\mathscr{A}||\mathscr{C}|^{1/2}, p\right\}.$$

Theorem 3.3.2. *Let $g_1,\dots,g_d \in \mathbb{F}[x,y]$ be quadratic polynomials, each of which has a non-zero xy-term. Then for $\mathscr{A} \subset \mathbb{F}$ we have*

$$\left|\sum_{i=1}^{d} g_i(\mathscr{A}\times\mathscr{A})\right| \gg \min\left\{|\mathscr{A}|^{2-\frac{1}{2^{d-1}}}, p\right\}.$$

Proof. Set $G_k(x_1,y_1\dots,x_k,y_k) = \sum_{i=1}^{k} g_i(x_i,y_i)$. We prove by induction on k that

$$\left|G_k(\mathscr{A}^{2k})\right| \gg \min\left\{|\mathscr{A}|^{2-\frac{1}{2^{k-1}}}, p\right\}.$$

The base case $k=1$ holds trivially. Suppose that the claim holds for some k with $1 \leq k < d$. Applying Corollary 3.3.1 with $g = g_{k+1}$ and $\mathscr{C} = G_k(\mathscr{A}^{2k})$ gives

$$|G_{k+1}(\mathscr{A}^{2(k+1)})| \gg \min\left\{|\mathscr{A}|\left(|\mathscr{A}|^{2-\frac{1}{2^{k-1}}}\right)^{1/2}, p\right\} = \min\left\{|\mathscr{A}|^{2-\frac{1}{2^{(k+1)-1}}}, p\right\}.$$

This proves the theorem. □

Theorem 3.1.4 follows immediately by setting $g_i = (x-y)^2$ for every i in Theorem 3.3.2. To prove Theorem 3.1.5, we merely have to start the induction at $k = 2$, and plug in the result of Guth and Katz [29].

Proof of Theorem 3.1.5. Set $\mathbb{F} = \mathbb{R}$. We prove $|\Delta(\mathscr{A}^d)| \gg |\mathscr{A}|^2/\log^{1/2^{d-2}}|\mathscr{A}|$ by induction on d. The base case $d = 2$ follows from the main result of [29], stated here as (3.1.1) in Section 3.1. Suppose that the claim holds for some $d > 2$. Applying Corollary 3.3.1 with $g = (x-y)^2$ and $C = \Delta(\mathscr{A}^d)$ gives

$$|\Delta(\mathscr{A}^{d+1})| \gg |\mathscr{A}||\Delta(\mathscr{A}^d)|^{1/2} \gg |\mathscr{A}|\left(\frac{|\mathscr{A}|^2}{\log^{1/2^{d-2}}|\mathscr{A}|}\right)^{1/2} = \frac{|\mathscr{A}|^2}{\log^{1/2^{(d+1)-2}}|\mathscr{A}|}.$$

This proves the theorem. □

Although this proof arose naturally from our general approach, it is worth noting that over $\mathbb{R}$ it is possible to prove the relevant case of Corollary 3.3.1 using only the Szemerédi-Trotter theorem [77], which leads to a proof of Theorem 3.1.5 without Theorem 8.2.1.

Alternative proof of Theorem 3.1.5. We define a point set and curve set by

$$\mathscr{P} := \mathscr{A} \times ((\mathscr{A}-\mathscr{A})^2 + \mathscr{C}), \quad \mathscr{S} := \{Y = (X-a)^2 + c : (a,c) \in \mathscr{A} \times \mathscr{C}\}.$$

The curves in $\mathscr{S}$ are parabolas, but we can apply the bijection $\varphi : (X,Y) \mapsto (X, Y - X^2)$, which sends the parabola $Y = X^2 - 2aX + a^2 + c$ to the line $Y' = -2aX' + a^2 + c$. Applying the Szemerédi-Trotter theorem [77] to the points $\varphi(\mathscr{P})$ and the lines $\varphi(\mathscr{S})$ gives

$$|\mathscr{A}|^2|C| \le \mathscr{I}(\varphi(\mathscr{P}), \varphi(\mathscr{S})) \ll (|\mathscr{A}||(\mathscr{A}-\mathscr{A})^2+\mathscr{C}|)^{2/3}(|\mathscr{A}||\mathscr{C}|)^{2/3} + |\mathscr{A}||(\mathscr{A}-\mathscr{A})^2+\mathscr{C}| + |\mathscr{A}||\mathscr{C}|.$$

It follows that $|(\mathscr{A}-\mathscr{A})^2 + \mathscr{C}| \gg |\mathscr{A}||\mathscr{C}|^{1/2}$.

We can now prove the theorem by induction exactly as in the previous proof. □

We are finished proving the main theorems in Section 3.1, but we give one more application that we find interesting.

Another polynomial in the form of Theorem 3.3.2 is the dot product function. For $P \subset \mathbb{F}^d$, define its *dot product set* by

$$\Pi(P) := \left\{ \sum_{i=1}^{d} x_i y_i : (x_1, \dots, x_d), (y_1, \dots, y_d) \in P \right\}.$$

Choosing $g_i = xy$ for every i in Theorem 3.3.2 gives $|\Pi(\mathscr{A}^d)| \gg \min\{|\mathscr{A}|^{2-\frac{1}{2^{d-1}}}, p\}$ for $\mathscr{A} \subset \mathbb{F}$. This bound was proved for $d = 2,3$ in [64]. More interestingly, we can prove that a better expansion bound holds for distances *or* for dot products (or for both).

Theorem 3.3.3. *For $\mathscr{A} \subset \mathbb{F}$ with $|\mathscr{A}| \ll p^{\frac{1}{2}+\frac{1}{5\cdot 2^{d-1}-2}}$ we have*

$$\max\left\{|\Pi(\mathscr{A}^d)|, |\Delta(\mathscr{A}^d)|\right\} \gg |\mathscr{A}|^{2-\frac{1}{5\cdot 2^{d-3}}}.$$

Proof. We prove the theorem by induction on d. For $d = 1$, we have $|\Delta(\mathscr{A})| \gg |\mathscr{A} - \mathscr{A}|$, so the statement follows from the sum-product bound

$$\max\{|\mathscr{A} - \mathscr{A}|, |\mathscr{A} \cdot \mathscr{A}|\} \gg |\mathscr{A}|^{6/5},$$

which was proved in [64] (also as a consequence of [66]). Assume that the claim holds for $d > 1$. If $|\Delta(\mathscr{A}^d)| \geq |\Pi(\mathscr{A}^d)|$, then we set $g = (x-y)^2$ and $\mathscr{C} = \Delta(\mathscr{A}^d)$, so that Corollary 3.3.1 gives

$$|\Delta(\mathscr{A}^{d+1})| = |g(\mathscr{A} \times \mathscr{A}) + \Delta(\mathscr{A}^d)| \gg |\mathscr{A}| \left(|\mathscr{A}|^{2-\frac{1}{5\cdot 2^{d-3}}}\right)^{1/2} = |\mathscr{A}|^{2-\frac{1}{5\cdot 2^{(d+1)-3}}}.$$

If $|\Pi(\mathscr{A}^d)| \geq |\Delta(\mathscr{A}^d)|$, then we set $g = xy$ and $\mathscr{C} = \Pi(\mathscr{A}^d)$, and do the same calculation. □

4 Distinct distances on regular varieties in finite spaces

4.1 Introduction

Let $\mathbb{F}_q$ be a finite field of order q, where q is a prime power. We denote the set of non-zero elements in $\mathbb{F}_q$ by $\mathbb{F}_q^*$. Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d$. For a polynomial $F(\mathbf{x}) \in \mathbb{F}_q[x_1,\dots,x_d]$ and an integer $k \geq 2$, we define

$$\Delta_{k,F}(\mathscr{E}) := \{F(\mathbf{x}_1 \pm \cdots \pm \mathbf{x}_k) : \mathbf{x}_i \in \mathscr{E},\ 1 \leq i \leq k\}.$$

When $k = 2$ and $F(\mathbf{x}) = x_1^2 + \cdots + x_d^2$, for the sake of simplicity, we use the notation $\Delta_2(\mathscr{E})$ instead of $\Delta_{2,F}(\mathscr{E})$. In this chapter, we are interested in the case when $\mathscr{E}$ is a subset in a *regular* variety. Let us first start with a definition of regular varieties which is taken from [19]

Definition 3. *For $\mathscr{E} \subseteq \mathbb{F}_q^d$, let $\mathbf{1}_{\mathscr{E}}$ denote the characteristic function on $\mathscr{E}$. Let $F(\mathbf{x}) \in \mathbb{F}_q[x_1,\dots,x_d]$ be a polynomial. The variety $\mathscr{V} := \{\mathbf{x} \in \mathbb{F}_q^d : F(\mathbf{x}) = 0\}$ is called a regular variety if $|\mathscr{V}| \approx q^{d-1}$ and $\widehat{\mathbf{1}_{\mathscr{V}}(\mathbf{m})} \ll q^{-(d+1)/2}$ for all $\mathbf{m} \in \mathbb{F}_q^d \setminus \mathbf{0}$, where*

$$\widehat{\mathbf{1}_{\mathscr{V}}(\mathbf{m})} = \frac{1}{q^d} \sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi(-\mathbf{m}\cdot\mathbf{x})\mathbf{1}_{\mathscr{V}}(\mathbf{x}).$$

There are several examples of regular varieties as follows:

1. Spheres of nonzero radii:

$$S_j = \left\{\mathbf{x} \in \mathbb{F}_q^d : ||\mathbf{x}|| = j\right\},\ j \in \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\} \quad [44]$$

2. A paraboloid:

$$P = \left\{\mathbf{x} \in \mathbb{F}_q^d : x_1^2 + \cdots + x_{d-1}^2 = x_d\right\} \quad [54]$$

3. Spheres defined by "Minkowski distance" with nonzero radii:

$$M_j = \left\{\mathbf{x} \in \mathbb{F}_q^d \colon x_1 \cdot x_2 \cdots x_d = j\right\}, \quad j \in \mathbb{F}_q^* \quad [36].$$

In 2007, Hart et al. [35], using Fourier analytic methods, made the first investigation on the distinct distances problem on the unit sphere in $\mathbb{F}_q^d$. In particular, they obtained the following.

Theorem 4.1.1 (**Hart et al.**, [35]). *For $\mathscr{E} \subseteq S_1$ in $\mathbb{F}_q^d$ with $d \geq 3$.*

1. *If $|\mathscr{E}| \geq Cq^{\frac{d}{2}}$ with a sufficiently large constant C, then there exists $c > 0$ such that $|\Delta_2(\mathscr{E})| \geq cq$.*
2. *If d is even and $|\mathscr{E}| \geq Cq^{\frac{d}{2}}$ with a sufficiently large constant C, then $\Delta_2(\mathscr{E}) = \mathbb{F}_q$.*
3. *If d is even, there exist $c > 0$ and $\mathscr{E} \subset S_1$ such that $|\mathscr{E}| \geq cq^{\frac{d}{2}}$ and $\Delta_2(\mathscr{E}) \neq \mathbb{F}_q$.*
4. *If d is odd and $|\mathscr{E}| \geq Cq^{\frac{d+1}{2}}$ with a sufficiently large constant $C > 0$, then $\Delta_2(\mathscr{E}) = \mathbb{F}_q$.*
5. *If d is odd, there exist $c > 0$ and $\mathscr{E} \subset S_1$ such that $|\mathscr{E}| \geq cq^{\frac{d+1}{2}}$ and $\Delta_2(\mathscr{E}) \neq \mathbb{F}_q$.*

Recently, Covert, Koh, and Pi [19] studied a generalization of Theorem 4.1.1, namely they dealt with the following question: How large does a subset $\mathscr{E}$ in a regular variety $\mathscr{V}$ need to be to make sure that $\Delta_k(\mathscr{E}) = \mathbb{F}_q$ or $|\Delta_k(\mathscr{E})| \gg q$.

The main idea in the proof of Theorem 4.1.1 is to reduce the distance problem to the dot product problem since the distance between two points $\mathbf{x}$ and $\mathbf{y}$ in S_1 is $2 - 2\mathbf{x} \cdot \mathbf{y}$, where $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_d y_d$. Therefore

$$|\Delta_2(\mathscr{E})| = |\Pi_2(\mathscr{E})| := \left|\left\{\mathbf{x} \cdot \mathbf{y} \colon \mathbf{x}, \mathbf{y} \in \mathscr{E}\right\}\right|. \tag{4.1.1}$$

For the case $k \geq 3$ and $\mathscr{E} \subset S_1$, one can check that

$$|\Delta_k(\mathscr{E})| = |\Pi_k(\mathscr{E})| := \left|\left\{\sum_{i=1}^{k}\sum_{j=1}^{k} a_{ij} \cdot b_{ij} \cdot \mathbf{x}^i \cdot \mathbf{x}^j \colon \mathbf{x}^l \in \mathscr{E}, 1 \leq l \leq k\right\}\right|,$$

where $a_{ij} = 1$ if $i < j$ and 0 otherwise, and $b_{ij} = 1$ for $i = 1$ and -1 otherwise.

However, it seems hard to get a good estimate on $|\Pi_k(\mathscr{E})|$ when $k \geq 3$, and if the unit sphere S_1 is replaced by a general regular variety $\mathscr{V}$, there is no guarantee that the

equality (4.1.1) will be satisfied. Thus, in general, we can not apply the approach of the proof of Theorem 4.1.1 to estimate the cardinality of $\Delta_k(\mathscr{E})$.

Using a new approach with Fourier analytic techniques, Covert, Koh and Pi [19] established that the condition on the cardinality of $\mathscr{E}$ in Theorem 4.1.1 can be improved to get $\Delta_k(\mathscr{E}) = \mathbb{F}_q$ with $k \geq 3$. The precise statement of their result is as follows.

Theorem 4.1.2 (**Covert et al.**, [19])**.** *Suppose that $\mathscr{V} \subset \mathbb{F}_q^d$ is a regular variety, and assume that $k \geq 3$ is an integer and $\mathscr{E} \subseteq \mathscr{V}$. If $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathscr{E}|)$, then we have*

$$\Delta_k(\mathscr{E}) \supseteq \mathbb{F}_q^* \text{ for even } d \geq 2,$$

and

$$\Delta_k(\mathscr{E}) = \mathbb{F}_q \text{ for odd } d \geq 3.$$

It follows from Theorem 4.1.1 that in order to get $\Delta_2(\mathscr{E}) = \mathbb{F}_q$, the sharp exponent of the sets $\mathscr{E}$ of S_1 must be $d/2$ for even $d \geq 4$, and $(d+1)/2$ for odd $d \geq 3$. Theorem 4.1.2 implies that the exponent $d/2$ can be decreased to $\frac{d-1}{2}+\frac{1}{k-1}$ for $k \geq 3$ and any regular variety $\mathscr{V} \subseteq \mathbb{F}_q^d$.

The main purpose of this chapter is to prove two generalizations of Theorem 4.1.2 by employing techniques from spectral graph theory. Our first result is the following.

Theorem 4.1.3. *Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^d$. Suppose that $\mathscr{V} \subset \mathbb{F}_q^d$ is a regular variety, and assume that $k \geq 3$ is an integer and $\mathscr{E} \subseteq \mathscr{V}$. If $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathscr{E}|)$, then for any $t \in \mathbb{F}_q^*$ we have*

$$\left|\left\{(\mathbf{x}_1,\dots,\mathbf{x}_k) \in \mathscr{E}^k \colon Q(\mathbf{x}_1+\cdots+\mathbf{x}_k) = t\right\}\right| = (1-o(1))\frac{|\mathscr{E}|^k}{q}.$$

Corollary 4.1.4. *Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^d$. Suppose that $\mathscr{V} \subset \mathbb{F}_q^d$ is a regular variety, and assume that $k \geq 3$ is an integer and $\mathscr{E} \subseteq \mathscr{V}$. If $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathscr{E}|)$, then we have*

$$\Delta_{k,Q}(\mathscr{E}) \supseteq \mathbb{F}_q^*.$$

Let $P(\mathbf{x}) = \sum_{j=1}^{d} a_j x_j^{s_j}$ be a diagonal polynomial in $\mathbb{F}_q[x_1,\dots,x_d]$ with $s_j \geq 2, \gcd(s_j,q) = 1$ and $a_j \neq 0$ for all $j = 1,\dots,d$. We obtain the following generalization of Theorem 4.1.2, which is inspired by [90].

Theorem 4.1.5. *Suppose that $V \subset \mathbb{F}_q^d$ is a regular variety, and assume that $k \geq 3$ is an integer and $\mathscr{E} \subseteq V$. For $X \subseteq \mathbb{F}_q$, if $|X||\mathscr{E}|^{2k-2} \gg q^{(d-1)(k-1)+2}$, we have*

$$|X + \Delta_{k,P}(\mathscr{E})| \gg q.$$

Corollary 4.1.6. *Suppose that $V \subset \mathbb{F}_q^d$ is a regular variety, and assume that $k \geq 3$ is an integer and $\mathscr{E} \subseteq V$. If $|\mathscr{E}| \gg q^{\frac{d-1}{2}+\frac{1}{k-1}}$, we have*

$$|\Delta_{k,P}(\mathscr{E})| \gg q.$$

The rest of this chapter is organized as follows: the proofs of Theorems 4.1.3 and 4.1.5 are presented in Sections 3 and 4, respectively.

4.2 Graph-theoretic tools

The following is the Expander Mixing Lemma which was mentioned in Chapter 2.

Lemma 4.2.1 ([32])**.** *Let $G = (V, E)$ be an (n, d, γ)-graph. The number of edges between two multi-sets of vertices B and C in G satisfies:*

$$\left| e_m(B,C) - \frac{d|B||C|}{n} \right| \leq \gamma \sqrt{\sum_{b \in B} m_B(b)^2} \sqrt{\sum_{c \in C} m_C(c)^2},$$

where $m_X(x)$ is the multiplicity of x in X.

Finite Euclidean graphs: Suppose Q is a non-degenerate quadratic form on $\mathbb{F}_q^d$. For any $\lambda \in \mathbb{F}_q \setminus \{0\}$, we define the finite Euclidean distance graph $E_q(d, Q, \lambda) = (V, E)$ as follows:

$$V\left(E_q(d,Q,\lambda)\right) = \mathbb{F}_q^d,\ (\mathbf{x},\mathbf{y}) \in E\left(E_q(d,Q,\lambda)\right) \Leftrightarrow\ Q(\mathbf{x}-\mathbf{y}) = \lambda.$$

The (n, d, γ) form of the graph $E_q(d, Q, \lambda)$ is estimated in the following theorem.

Theorem 4.2.2. ***[Bannai et al.*** *[2], Kwok [50]] Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^d$. For any $\lambda \in \mathbb{F}_q \setminus \{0\}$, the graph $E_q(d, Q, \lambda)$ is an $(q^d, (1 + o(1))q^{d-1}, 2q^{\frac{d-1}{2}})$-graph.*

For a directed graph G on n vertices, such that both the inner and outer degree of each vertex are d, we denote its adjacency matrix by A_G. Recall that A_G is defined

as the matrix with entries a_{ij}, where $a_{ij} = 1$ if there is a directed edge from i to j, and zero otherwise. We denote by $\gamma_1(G), \ldots, \gamma_n(G)$ the eigenvalues of A_G. Since the eigenvalues of G might have complex values, we cannot order them. However, for any $1 \le i \le n$, $|\gamma_i| \le d$. Define $\gamma_1(G) := d, \gamma(G) := \max_{|\gamma_i(G)| \ne d} |\gamma_i(G)|$. We will use the term of digraph for a directed graph.

We say that an $n \times n$ matrix A is *normal* if $A^t A = AA^t$, where A^t is the transpose of A.

Let G be a digraph, we say that G is normal if A_G is a normal matrix. One can easily check that G is normal if and only if $|N^+(u,v)| = |N^-(u,v)|$ for any two vertices u and v, where $N^+(u,v)$ is the set of vertices w such that $\overrightarrow{uw}, \overrightarrow{vw}$ are edges, and $N^-(u,v)$ is the set of vertices w such that $\overrightarrow{wu}, \overrightarrow{wv}$ are edges.

We say that a directed graph G is an (n,d,γ)-*digraph* if it has n vertices, both the inner and the outer degree of each vertex are d, $\gamma(G) \le \gamma$, and it is normal.

Let G be an (n,d,γ)-digraph. For any two vertex subsets U and W of G, let $e(U,W)$ be the number of ordered pairs $(u,w) \in U \times W$ such that $\overrightarrow{uw}$ is an edge of G. Vu [95] developed a directed version of the Expander Mixing Lemma as follows.

Lemma 4.2.3 (**Vu**, [95])**.** *Let $G = (V,E)$ be an (n,d,γ)-digraph. For any two sets $B, C \subset V$, we have*

$$\left| e(B,C) - \frac{d}{n}|B||C| \right| \le \gamma \sqrt{|B||C|}.$$

By using similar arguments as in the proofs of [32, Lemma 16] and [95, Lemma 3.1], we obtain the multiplicity version of Lemma 4.2.3.

Lemma 4.2.4 (Multiplicity version)**.** *Let $G = (V,E)$ be an (n,d,γ)-digraph. For any two multi-sets B and C of vertices , we have*

$$\left| e(B,C) - \frac{d}{n}|B||C| \right| \le \gamma \sqrt{\sum_{b \in B} m_B(b)^2} \sqrt{\sum_{c \in C} m_C(c)^2},$$

where $m_X(x)$ is the multiplicity of x in X.

We leave the proof of Lemma 4.2.4 to the interested reader.

4.3 Proof of Theorem 4.1.3

Let H be a finite (additive) abelian group and S be a subset of H. Define a directed Cayley graph C_S as follows. The vertex set of C_S is H. There is a directed edge from x

to y if and only if $y-x \in S$. It is clear that every vertex C_S has out-degree $|S|$. Let φ_α, $\alpha \in H$, be the additive charaters of H. It is well known that for any $\alpha \in H$, $\sum_{s\in S}\varphi_\alpha(s)$ is an eigenvalue of C_S, with respect the eigenvector $(\varphi_\alpha(x))_{x\in H}$.

Let $\mathcal{V}$ be a regular variety defined by

$$\mathcal{V} := \{\mathbf{x} \in \mathbb{F}_q^d \colon F(\mathbf{x}) = 0\},$$

for some polynomial $F \in \mathbb{F}_q[x_1, \ldots, x_d]$.

The Cayley graph $C_\mathcal{V}$ is defined with $H = \mathbb{F}_q^d$ and $S = \mathcal{V}$. In particular, the edge set of the Cayley graph $C_\mathcal{V}$ is defined by

$$E(C_\mathcal{V}) = \{\overrightarrow{(u,v)} \in H \times H \colon v - u \in \mathcal{V}\}.$$

For any two vertices u and v in H, we have

$$|N^+(u,v)| = |N^-(u,v)| = |(u+\mathcal{V}) \cap (v+\mathcal{V})|,$$

which implies that $C_\mathcal{V}$ is normal. We now study the (n,d,γ) form of this digraph in the next theorem.

Theorem 4.3.1. *The Cayley graph $C_\mathcal{V}$ is an $\left(q^d, |\mathcal{V}|, cq^{\frac{d-1}{2}}\right)$-digraph for some positive constant c.*

Proof. It is clear that the graph $C_\mathcal{V}$ has q^d vertices and the in-degree and out-degree of each vertex are both $|\mathcal{V}|$. Next, we will estimate eigenvalues of the graph $C_\mathcal{V}$. It is well-known that the exponentials (or characters of the additive group $\mathbb{F}_q^d$)

$$\varphi_\mathbf{m}(\mathbf{x}) = \varphi(\mathbf{x}\cdot\mathbf{m}), \tag{4.3.1}$$

for $\mathbf{x}, \mathbf{m} \in \mathbb{F}_q^d$, are eigenfunctions of the adjacency operator for the graph $C_\mathcal{V}$ corresponding to the eigenvalue

$$\begin{aligned}
\lambda_\mathbf{m} &= \sum_{\mathbf{x}\in\mathcal{V}} \varphi_\mathbf{m}(\mathbf{x}) \\
&= \sum_{\mathbf{x}\in\mathcal{V}} \varphi(\mathbf{x}\cdot\mathbf{m}) \\
&= q^d \widehat{\mathbf{1}_\mathcal{V}(-\mathbf{m})} \\
&\ll q^{(d-1)/2},
\end{aligned}$$

when $\mathbf{m} \neq \mathbf{0}$. If $\mathbf{m} = \mathbf{0}$, then $\lambda_{\mathbf{0}} = |\mathcal{V}|$, which is the largest eigenvalue of $C_{\mathcal{V}}$. In other words, $C_{\mathcal{V}}$ is an $\left(q^d, |\mathcal{V}|, cq^{\frac{d-1}{2}}\right)$-digraph for some positive constant c. □

In order to prove Theorem 4.1.3, we need the following notations.

For an even integer $k = 2m \geq 2$ and $\mathscr{E} \subset \mathbb{F}_q^d$, *the k-energy* is defined by

$$\Lambda_k(\mathscr{E})L = \left|\left\{(\mathbf{x}^1, \ldots, \mathbf{x}^k) \in \mathscr{E}^k \colon \mathbf{x}^1 + \cdots + \mathbf{x}^m = \mathbf{x}^{m+1} + \cdots + \mathbf{x}^k\right\}\right|.$$

For $\mathscr{E} \subseteq \mathbb{F}_q^d$, we define

$$\nu_k(t) := \left|\left\{(\mathbf{x}^1, \ldots, \mathbf{x}^k) \in \mathscr{E}^k \colon Q(\mathbf{x}^1 + \cdots + \mathbf{x}^k) = t\right\}\right|.$$

In our next lemmas, we give estimates on the magnitude of $\nu_k(t)$.

Lemma 4.3.2. *For $\mathscr{E} \subset \mathbb{F}_q^d$ and $k \geq 2$ even, we have*

$$\left|\nu_k(t) - (1 + o(1))\frac{|\mathscr{E}|^k}{q}\right| \leq q^{(d-1)/2}\Lambda_k(\mathscr{E})$$

.

Proof. Suppose that $k = 2m$. Let $\mathscr{A}$ and $\mathscr{B}$ be multi-sets of points in $\mathbb{F}_q^d$ defined as follows

$$\mathscr{A} := \{\mathbf{x}_1 + \cdots + \mathbf{x}_m \colon \mathbf{x}_i \in \mathscr{E}, 1 \leq i \leq m\}, \quad \mathscr{B} := \{-\mathbf{x}_{m+1} - \cdots - \mathbf{x}_k \colon \mathbf{x}_i \in \mathscr{E}, m+1 \leq i \leq k\}.$$

It is easy to check that

$$\sum_{\mathbf{a} \in \mathscr{A}} m_{\mathscr{A}}(\mathbf{a})^2 = \Lambda_k(\mathscr{E}), \quad \sum_{\mathbf{b} \in \mathscr{B}} m_{\mathscr{B}}(\mathbf{b})^2 = \Lambda_k(\mathscr{E}),$$

and $\nu_k(t)$ is equal to the number of edges between $\mathscr{A}$ and $\mathscr{B}$ in the graph $E_q(d, Q, t)$. Thus the lemma follows immediately from Lemma 4.2.1 and Theorem 4.2.2. □

By using the same techniques, we get a similar result for the case k odd.

Lemma 4.3.3. *For $\mathscr{E} \subset \mathbb{F}_q^d$ and $k \geq 3$ odd, we have*

$$\left|\nu_k(t) - (1 + o(1))\frac{|\mathscr{E}|^k}{q}\right| \leq 2q^{(d-1)/2}\left(\Lambda_{k-1}(\mathscr{E})\right)^{1/2}\left(\Lambda_{k+1}(\mathscr{E})\right)^{1/2}.$$

Combining Lemmas 4.3.2 and 4.3.3 leads to the following theorem.

Theorem 4.3.4. *Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d$. Then we have*

1. *If $q^{\frac{d+1}{2}}\Lambda_k(\mathscr{E}) = o(|\mathscr{E}|^k)$ and k is even, then*

$$\left|\left\{(\mathbf{x}_1,\dots,\mathbf{x}_k)\in\mathscr{E}^k\colon Q(\mathbf{x}_1+\cdots+\mathbf{x}_k)=t\right\}\right| = (1+o(1))\frac{|\mathscr{E}|^k}{q}.$$

2. *If $q^{\frac{d+1}{2}}(\Lambda_{k-1}(\mathscr{E}))^{1/2}(\Lambda_{k+1}(\mathscr{E}))^{1/2} = o(|\mathscr{E}|^k)$ and k is odd, then*

$$\left|\left\{(\mathbf{x}_1,\dots,\mathbf{x}_k)\in\mathscr{E}^k\colon Q(\mathbf{x}_1+\cdots+\mathbf{x}_k)=t\right\}\right| = (1+o(1))\frac{|\mathscr{E}|^k}{q}.$$

Theorem 4.3.4 implies that in order to prove Theorem 4.1.3, it is sufficient to bound $\Lambda_k(\mathscr{E})$.

Lemma 4.3.5. *For a regular variety $\mathscr{V}\subset\mathbb{F}_q^d$. If $k\geq 4$ is even, and $\mathscr{E}\subset\mathscr{V}$, we have*

$$\left|\Lambda_k(\mathscr{E}) - (1+o(1))\frac{|\mathscr{E}|^{k-1}}{q}\right| \ll q^{(d-1)/2}(\Lambda_{k-2}(\mathscr{E}))^{1/2}(\Lambda_k(\mathscr{E}))^{1/2}.$$

Proof. Since $\mathscr{E}$ is a subset in the variety $\mathscr{V}$, we have the following estimate

$$\Lambda_k(\mathscr{E}) \leq \sum_{\mathbf{x}_1,\dots,\mathbf{x}_{k-1}\in\mathscr{E}} \mathbf{1}_{\mathscr{V}}(\mathbf{x}_1+\cdots+\mathbf{x}_{k/2}-\mathbf{x}_{k/2+1}-\cdots-\mathbf{x}_{k-1}).$$

Let $\mathscr{A}$ and $\mathscr{B}$ be two multi-sets defined by

$$\mathscr{A} := \{\mathbf{x}_1+\cdots+\mathbf{x}_{k/2}\colon \mathbf{x}_i\in\mathscr{E}, 1\leq i\leq k/2\},$$

and

$$\mathscr{B} := \{-\mathbf{x}_{k/2+1}-\cdots-\mathbf{x}_{k-1}\colon \mathbf{x}_i\in\mathscr{E}, k/2+1\leq i\leq k-1\}.$$

It is clear that

$$\sum_{\mathbf{a}\in\mathscr{A}} m_{\mathscr{A}}(\mathbf{a})^2 = \Lambda_k(\mathscr{E}), \quad \sum_{\mathbf{b}\in\mathscr{B}} m_{\mathscr{B}}(\mathbf{b})^2 = \Lambda_{k-2}(\mathscr{E}).$$

On the other hand, $\Lambda_k(\mathscr{E})$ is equal to the number of edges between $\mathscr{A}$ and $\mathscr{B}$ in the Cayley graph $C_{\mathscr{V}}$. Thus the lemma follows from Lemmas 4.2.4 and 4.3.1. □

For $\mathscr{E} \subseteq \mathscr{V}$ and $k \geq 4$ even, it follows from Lemma 4.3.5 that

$$\Lambda_k(\mathscr{E}) \ll \frac{|\mathscr{E}|^{k-1}}{q} + q^{(d-1)/2}(\Lambda_{k-2}(\mathscr{E}))^{1/2}(\Lambda_k(\mathscr{E}))^{1/2}.$$

Solving this inequality in terms of $\Lambda_k(\mathscr{E})$ gives us

$$\Lambda_k(\mathscr{E}) \ll q^{d-1}\Lambda_{k-2}(\mathscr{E}) + \frac{|\mathscr{E}|^{k-1}}{q}.$$

Using inductive arguments, we obtain the following estimate for $\mathscr{E} \subseteq \mathscr{V}$ and $k \geq 4$ even

$$\Lambda_k(\mathscr{E}) \ll q^{\frac{(d-1)(k-2)}{2}}\Lambda_2(\mathscr{E}) + \frac{|\mathscr{E}|^{k-1}}{q}\sum_{j=0}^{(k-4)/2}\left(\frac{q^{d-1}}{|\mathscr{E}|^2}\right)^j. \tag{4.3.2}$$

If we assume that $|\mathscr{E}| > q^{(d-1)/2}$, then the inequality (4.3.2) implies the following theorem.

Theorem 4.3.6. *Let $\mathscr{E}$ be a subset of a regular variety $\mathscr{V}$ in $\mathbb{F}_q^d$ with $|\mathscr{E}| > q^{(d-1)/2}$.*

1. *If $k \geq 2$ is even, then*
$$\Lambda_k(\mathscr{E}) \ll q^{\frac{(d-1)(k-2)}{2}}|\mathscr{E}| + \frac{|\mathscr{E}|^{k-1}}{q}.$$
2. *If $k \geq 3$ is odd, then*
$$\Lambda_{k-1}(\mathscr{E})\Lambda_{k+1}(\mathscr{E}) \ll q^{(d-1)(k-2)}|\mathscr{E}|^2 + q^{\frac{(d-1)(k-3)-2}{2}}|\mathscr{E}|^{k+1} + \frac{|\mathscr{E}|^{2k-2}}{q^2}.$$

Note that the first statement of Theorem 4.3.6 follows from (4.3.2) with the facts that $\Lambda_2(\mathscr{E}) = |\mathscr{E}|$ and $\frac{q^{d-1}}{|\mathscr{E}|^2} < 1$, and the second is a consequence of the first one.

We are now ready to prove Theorem 4.1.3.

Proof of Theorem 4.1.3. We now consider two following cases:

Case 1: If $k \geq 2$ is even and $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathscr{E}|)$, then it follows from Theorem 4.3.6 that

$$q^{\frac{d+1}{2}}\Lambda_k(\mathscr{E}) = o(|\mathscr{E}|^k).$$

Case 2: If $k \geq 3$ is odd and $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathscr{E}|)$, then it follows from Theorem 4.3.6 that

$$q^{\frac{d+1}{2}}(\Lambda_{k-1}(\mathscr{E}))^{1/2}(\Lambda_{k+1}(\mathscr{E}))^{1/2} = o(|\mathscr{E}|^k).$$

In other words, Theorem 4.1.3 follows immediately from Theorem 4.3.4.

□

4.4 Proof of Theorem 4.1.5

To prove Theorem 4.1.5, we need to construct a new Cayley graph as follows.

Let $P(\mathbf{x}) = \sum_{j=1}^{d} a_j x_j^{s_j}$ be a diagonal polynomial in $\mathbb{F}_q[x_1,\ldots,x_d]$ with $s_j \geq 2, \gcd(s_j, q) = 1$ and $a_j \neq 0$ for all $j = 1,\ldots,d$, and

$$P'(x_1,\ldots,x_{2d}) = P(x_1,\ldots,x_d) - P(x_{d+1},\ldots,x_{2d}) \in \mathbb{F}_q[x_1,\ldots,x_{2d}].$$

We define the graph $C_{P'}(\mathbb{F}_q^{2d+1})$ to be the Cayley graph with $H = \mathbb{F}_q \times \mathbb{F}_q^{2d}$ and $S = \{(x_0,\mathbf{x}) \in \mathbb{F}_q \times \mathbb{F}_q^{2d} \mid x_0 + P'(\mathbf{x}) = 0\}$, i.e.

$$E(C_{P'}(\mathbb{F}_q^{2d+1})) = \left\{\overrightarrow{((x_0,\mathbf{x}),(y_0,\mathbf{y}))} \in H \times H \colon y_0 - x_0 + P'(\mathbf{y}-\mathbf{x}) = 0\right\}.$$

The (n,d,γ) form of $C_{P'}(\mathbb{F}_q^{2d+1})$ was studied in [90].

Lemma 4.4.1 ([90])**.** *For any odd prime power q, $d \geq 1$, then $C_{P'}(\mathbb{F}_q^{2d+1})$ is an*

$$\left(q^{2d+1}, q^{2d}, q^d\right) - \textit{digraph.}$$

For $\mathscr{E} \subseteq \mathbb{F}_q^d$ and $X \subseteq \mathbb{F}_q$, define

$$\nu_{P,k}(t) := \left|\{(a,\mathbf{x}_1,\ldots,\mathbf{x}_k) \in X \times \mathscr{E}^k \colon a + P(\mathbf{x}_1+\cdots+\mathbf{x}_k) = t\}\right|.$$

Our next lemmas are the main steps in the proof of Theorem 4.1.5.

Lemma 4.4.2. *For $\mathscr{E} \subseteq \mathbb{F}_q^d$ and $k \geq 2$ even, we have the following estimate*

$$\sum_{t\in\mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|\mathscr{E}|^{2k}|X|^2}{q} + q^d|X|\Lambda_k(\mathscr{E})^2.$$

Proof. Let $\mathscr{A}$ and $\mathscr{B}$ be multi-sets defined by:

$$\mathscr{A} := \{(a, -\mathbf{x}_1 - \cdots - \mathbf{x}_{k/2}, -\mathbf{y}_1 - \cdots - \mathbf{y}_{k/2}) \colon a \in X, \mathbf{x}_i, \mathbf{y}_i \in \mathscr{E}\},$$

and

$$\mathscr{B} := \{(b, \mathbf{x}_{k/2+1} + \cdots + \mathbf{x}_k, \mathbf{y}_{k/2+1} + \cdots + \mathbf{y}_{k/2+1}) \colon b \in X, \mathbf{x}_i, \mathbf{y}_i \in \mathscr{E}\}.$$

One can check that

$$\sum_{\mathbf{x}\in\mathscr{A}} m_{\mathscr{A}}(\mathbf{x})^2 = |X|\Lambda_k(\mathscr{E})^2, \ \sum_{\mathbf{x}\in\mathscr{B}} m_{\mathscr{B}}(\mathbf{x})^2 = |X|\Lambda_k(\mathscr{E})^2, \ |\mathscr{A}| = |\mathscr{B}| = |X||\mathscr{E}|^k.$$

On the other hand, it is clear that $\sum_{t\in\mathbb{F}_q} \nu_{P,k}^2$ is equal to the number of edges from $\mathscr{A}$ to $\mathscr{B}$ in the graph $C_{P'}(\mathbb{F}_q^{2d+1})$. Thus it follows from Lemma 4.2.4 and Theorem 4.4.1 that

$$\sum_{t\in\mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|\mathscr{E}|^{2k}|X|^2}{q} + q^d|X|\Lambda_k(\mathscr{E})^2.$$

This ends the proof of the lemma. □

By employing the same techniques, we get a similar result for the case $k \geq 3$ odd.

Lemma 4.4.3. *For $\mathscr{E} \subseteq \mathbb{F}_q^d$ and $k \geq 3$ odd, we have the following estimate*

$$\sum_{t\in\mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|\mathscr{E}|^{2k}|X|^2}{q} + q^d|X|\Lambda_{k-1}(\mathscr{E})\Lambda_{k+1}(\mathscr{E}).$$

We are now ready to prove Theorem 4.1.5.

Proof of Theorem 4.1.5. It follows from the proof of Theorem 2.6 in [90] that

$$|X + \Delta_{k,P}(\mathscr{E})| \gg \frac{|X|^2|\mathscr{E}|^{2k}}{\sum_{t\in\mathbb{F}_q} \nu_{P,k}(t)^2}.$$

Therefore from Lemma 4.4.2 and Lemma 4.4.3, we get two following cases:

1. If $k \geq 2$ is even, we obtain

$$|X + \Delta_{k,P}(\mathscr{E})| \gg \min\left\{\frac{|X||\mathscr{E}|^{2k}}{q^d\Lambda_k(\mathscr{E})^2}, q\right\}.$$

2. If $k \geq 3$ is odd, we obtain

$$|X + \Delta_{k,P}(\mathscr{E})| \gg \min\left\{\frac{|X||\mathscr{E}|^{2k}}{q^d \Lambda_k(\mathscr{E})\Lambda_{k-1}(\mathscr{E})}, q\right\}.$$

Thus Theorem 4.1.5 follows immediately from Theorem 4.3.6, which concludes the proof of the theorem. □

5 Point-sphere incidences in finite spaces

5.1 Introduction

Let $\mathbb{F}_q$ be a finite field of q elements where q is a large odd prime power. Let P be a set of points, L a set of lines over $\mathbb{F}_q^d$, and $I(P,L)$ the number of incidences between P and L. Bourgain, Katz, and Tao [9] proved that for any $0 < \alpha < 2$ and $|P|, |L| \leq N = q^\alpha$, $I(P,L) \ll N^{3/2-\varepsilon}$, where $\varepsilon = \varepsilon(\alpha)$. By employing the Erdős-Rényi graph (see 2.1 for the definition), Vinh [85] improved this bound in the case $1 \leq \alpha \leq 2$, and gave the following estimate.

Theorem 5.1.1. *Let $\mathscr{P}$ be a set of points and $\mathscr{L}$ a set of lines in $\mathbb{F}_q^2$. Then we have*

$$I(\mathscr{P},\mathscr{L}) \leq \frac{|\mathscr{P}||\mathscr{L}|}{q} + q^{1/2}\sqrt{|\mathscr{P}||\mathscr{L}|}.$$

The above result was also proved for points and hyperplanes, and for points and k-subspaces (see [7, 85] for more details).

Let $P = a_1 x_1^{c_1} + \cdots + a_d x_d^{c_d} \in \mathbb{F}_q[x_1, \ldots, x_d]$, where $2 \leq c_i \leq N$, for some constant $N > 0$, $\gcd(c_i, q) = 1$, and $a_i \in \mathbb{F}_q$ for all $1 \leq i \leq d$. We define the *generalized sphere*, or *P-sphere*, centered at $b = (b_1, \ldots, b_d)$ of radius $r \in \mathbb{F}_q$ to be the set $\{x \in \mathbb{F}_q^d \mid P(x-b) = r\}$.

Let $\mathscr{P}$ be a set of points in $\mathbb{F}_q^d$ and $\mathscr{S}$ be a set of P-spheres with arbitrary radii in $\mathbb{F}_q^d$. The number of incidences between $\mathscr{P}$ and $\mathscr{S}$, which is denoted by $I(\mathscr{P},\mathscr{S})$, is the cardinality of $\{(p,s) \in \mathscr{P} \times \mathscr{S} : \ p \in s\}$.

The main purpose of this chapter is to give a similar bound on the number of incidences between points and generalized spheres by employing the spectral graph method. With the same method, we also consider some related problems in Sections 4 and 5. Our main result is the following.

Theorem 5.1.2. *Let $\mathscr{P}$ be a set of points and $\mathscr{S}$ a set of P-spheres with arbitrary radii in $\mathbb{F}_q^d$. Then the number of incidences between points and spheres satisfies*

$$\left| I(\mathscr{P},\mathscr{S}) - \frac{|\mathscr{P}||\mathscr{S}|}{q} \right| \leq q^{d/2}\sqrt{|\mathscr{P}||\mathscr{S}|}. \tag{5.1.1}$$

In the case $P(x) = \sum_{i=1}^{d} x_i^2$, Cilleruelo et al. [15] have independently proved (5.1.1). In this case, we also obtain a similar estimate over finite rings (see [82] for the Szemerédi-Trotter theorem over finite rings).

Theorem 5.1.3. *Let $\mathscr{P}$ be a set of points and $\mathscr{S}$ a set of spheres with arbitrary radii in $\mathbb{Z}_q^d$, q is an odd integer. Then the number of incidences between points and spheres satisfies*

$$\left| I(\mathscr{P},\mathscr{S}) - \frac{|\mathscr{P}||\mathscr{S}|}{q} \right| \leq \sqrt{2\tau(q)}\frac{q^d}{\gamma(q)^{d/2}}\sqrt{|\mathscr{P}||\mathscr{S}|},$$

where $\gamma(q)$ is the smallest prime divisor of q, and $\tau(q)$ the number of divisors of q.

Generalized pinned distances: Let $F(x) \in \mathbb{F}_q[x_1,\dots,x_d]$ be a polynomial and $\mathscr{E} \subset \mathbb{F}_q^d$. Given $x \in \mathbb{F}_q^d$, we denote the pinned F-distance set determined by $\mathscr{E}$ and x by

$$\Delta_F(\mathscr{E},x) = \{F(y-x) \in \mathbb{F}_q \mid y \in \mathscr{E}\}.$$

We are interested in finding the elements $x \in \mathbb{F}_q^d$ and the size of $\mathscr{E} \subset \mathbb{F}_q^d$ such that $\Delta_F(\mathscr{E},x) \gtrsim q$. In the case $F(x) = x_1^2 + \cdots + x_d^2$, Chapman et al. [12] proved that for any subset $\mathscr{E} \subset \mathbb{F}_q^d$ such that $|\mathscr{E}| \geq q^{(d+1)/2}$, there exists a subset $\mathscr{E}' \subset \mathscr{E}$ such that $|\mathscr{E}'| \sim |\mathscr{E}|$, and for every $y \in \mathscr{E}'$ we have $|\Delta_F(\mathscr{E},y)| > \frac{q}{2}$. Cilleruelo et al. [15] reproved the same result using their bound on number of incidences between points and spheres.

In this general setting, the main difficulty in this problem is that we do not know the explicit form of the polynomial $F(x)$. Koh and Shen [45] found some conditions on $F(x)$ to obtain the desired bound. We remark that if F is a diagonal polynomial of the form $\sum_{j=1}^{d} a_j x_j^s$, the conditions of Koh and Shen are satisfied. However, if we consider the polynomial $F(x) = P(x) = \sum_{j=1}^{d} a_j x_j^{c_j}$, where the exponents c_j are distinct, then we have not found any reference which shows that those conditions are satisfied.

As a consequence of Theorem 5.1.2, the following result can be derived in a similar way to how [15] derived their result from their bound on the number of incidences between points and spheres. It generalizes the pinned distance results of [12].

Theorem 5.1.4. *Let $\mathscr{E} \subset \mathbb{F}_q^d$ with $|\mathscr{E}| > \sqrt{(1-c^2)/c^4}\cdot q^{(d+1)/2}$ for some $0 < c < 1$. Then the number of points $p \in \mathscr{E}$ satisfying $|\Delta_P(\mathscr{E},p)| > (1-c)q$ is at least $(1-c)|\mathscr{E}|$.*

Incidences between a random point set and a random P-sphere set: It follows from Theorem 5.1.2 that if $\mathscr{P}$ is a set of points and $\mathscr{S}$ is a set of P-spheres such that $|\mathscr{P}||\mathscr{S}| > q^{d+2}$, then there exists at least one incidence pair $(p,s) \in \mathscr{P} \times \mathscr{S}$ with $p \in s$. We improve the bound q^{d+2} in the sense that for any $\alpha \in (0,1)$ it suffices to take $t \geq C_\alpha q$ randomly chosen points and spheres over $\mathbb{F}_q^d$ to guarantee that the probability of no incidences is exponentially small, namely α^t, when q is large enough. We remark that the ideas in this part are similar to the case between points and lines in [91]. More precisely, our result is the following.

Theorem 5.1.5. *For any $\alpha > 0$, there exists an integer $q_0 = q_0(\alpha)$ and a number $C_\alpha > 0$ with the following property. When a point set $\mathscr{P}$ and a P-sphere set $\mathscr{S}$ where $|\mathscr{P}| = |\mathscr{S}| = t \geq C_\alpha q$ are chosen randomly in $\mathbb{F}_q^d$, the probability of $\{(p,s) \in \mathscr{P} \times \mathscr{S} : p \in s\} = \emptyset$ is at most α^t, provided that $q \geq q_0$.*

Generalized isosceles triangles: Given a set $\mathscr{E}$ of n points in $\mathbb{R}^2$, let $h(\mathscr{E})$ be the number of isosceles triangles determined by $\mathscr{E}$. Define $h(n) = \min_{|\mathscr{E}|=n} h(\mathscr{E})$. Pach and Tardos [59] proved that $h(n) = O(n^{2.136})$. In this chapter, we consider the finite field version of this problem. Let us give some notation: A *P-isosceles triangle* at a vertex x is a triple of distinct elements $(x,y,z) \in \mathbb{F}_q^d \times \mathbb{F}_q^d \times \mathbb{F}_q^d$ such that $P(x-y) = P(x-z)$. We will show that for any subset $\mathscr{E}$ in $\mathbb{F}_q^d$ such that its cardinality is large enough, the number of isosceles triangles determined by $\mathscr{E}$ is $(1+o(1))|\mathscr{E}|^3/q$.

Theorem 5.1.6. *Given a set of n points $\mathscr{E}$ in $\mathbb{F}_q^d$, $d \geq 2$. If $|\mathscr{E}| \gg q^{\frac{2(d+1)}{3}}$, then the number of isosceles triangles determined by $\mathscr{E}$ is $(1+o(1))|\mathscr{E}|^3/q$.*

Distinct distances subset: Given a set $\mathscr{E}$ of n points in $\mathbb{R}^2$, let $g(\mathscr{E})$ be the maximal cardinality of a subset U in $\mathscr{E}$ such that no distance determined by U occurs twice. Define $g(n) = \min_{|\mathscr{E}|=n} g(\mathscr{E})$. Charalambides [13] proved that $n^{1/3}/(\log n) \lesssim g(n) \lesssim n^{1/2}/(\log n)^{1/4}$, where the upper bound is obtained from the Erdős distinct distances problem (see [16, 51] for more details, earlier results, and results in higher dimensions). In this chapter, we study the finite field analogue of this problem.

Given a set of n points $\mathscr{E} \subset \mathbb{F}_q^d$, a subset $U \subset \mathscr{E}$ is called a *distinct P-distances subset* if there are no four distinct points $x,y,z,t \in U$ such that $P(x-y) = P(z-t)$. Using the same method that Thiele used in $\mathbb{R}^2$ (see [58, p.191] for more details), we show that for any large enough set $\mathscr{E}$ in $\mathbb{F}_q^d$, there exists a distinct P-distances subset of cardinality at least $Cq^{1/3}$, for some constant C. More precisely, we have the following estimate.

Theorem 5.1.7. *Let $\mathscr{E} \subset \mathbb{F}_q^d$, $d \geq 2$, $|\mathscr{E}| \gg q^{2(d+1)/3}$. If $U_P \subset \mathscr{E}$ is a maximal distinct P-distances subset of $\mathscr{E}$, then $q^{1/3} \ll |U_P| \ll q^{1/2}$.*

5.2 Graph-theoretic tools

The following is the Expander Mixing Lemma for (n,d,γ)-graph, which has been mentioned in Chapter 2.

Lemma 5.2.1. *Let $G=(V,E)$ be an (n,d,γ)-graph. For any two sets $B,C\subset V$, we have*

$$\left|e(B,C)-\frac{d|B||C|}{n}\right|\leq\gamma\sqrt{|B||C|}.$$

In order to prove Theorem 5.1.3, we use the *sum-product graph* defined as the following. The vertex set of the sum-product graph $\mathcal{SP}(\mathbb{Z}_q^{d+1})$ is the set $V(\mathcal{SP}(\mathbb{Z}_q^{d+1}))=\mathbb{Z}_q\times\mathbb{Z}_q^d$. Two vertices $U=(a,\mathbf{b})$ and $V=(c,\mathbf{d})\in V(\mathcal{SP}(\mathbb{Z}_q^{d+1}))$ are connected by an edge, $(U,V)\in E(\mathcal{SP}(\mathbb{Z}_q^{d+1}))$, if and only if $a+c=\mathbf{b}\cdot\mathbf{d}$. Our construction is similar to that of Solymosi in [73]. We have the following lemma about the spectrum of the sum-product graph $\mathcal{SP}(\mathbb{Z}_q^{d+1})$ (see [94, Lemma 4.1] for the proof).

Lemma 5.2.2. *For any $d\geq 1$, the sum-product graph $\mathcal{SP}(\mathbb{Z}_q^{d+1})$ is an*

$$\left(q^{d+1},q^d,\sqrt{2\tau(q)}\frac{q^d}{\gamma(q)^{d/2}}\right)-\textit{graph.}$$

However, it seems difficult to use the spectrum of an undirected graph to analyze the number of incidences between points and P-spheres, where $Q(x)\in\mathbb{F}_q[x_1,\ldots,x_d]$ is an arbitrary diagonal polynomial. We will introduce some Cayley graphs to deal with this problem. First we have to recall the Expander Mixing Lemma for directed graphs, which was presented in Chapter 4.

Lemma 5.2.3. *Let $G=(V,E)$ be a (n,d,γ)-digraph. For any two sets $B,C\subset V$, we have*

$$\left|e(B,C)-\frac{d|B||C|}{n}\right|\leq\gamma\sqrt{|B||C|}.$$

Let H be a finite abelian group and S a subset of H. The *Cayley graph* is the digraph $C_S(H)=(H,E)$, where the vertex set is H, and there is a directed edge from vertex x to vertex y if and only if $y-x\in S$. It is clear that every vertex of $C_S(H)$ has out-degree $|S|$. We define the graph $C_P(\mathbb{F}_q^{d+1})$ to be the Cayley graph with $H=\mathbb{F}_q\times\mathbb{F}_q^d$ and $S=\{(x_0,x)\in\mathbb{F}_q\times\mathbb{F}_q^d\mid x_0+P(x)=0\}$, i.e.

$$E(C_P(\mathbb{F}_q^{d+1}))=\{((x_0,x),(y_0,y))\in H\times H\mid x_0-y_0+P(x-y)=0\}.$$

We have the following result on the spectrum of $C_P(\mathbb{F}_q^{d+1})$.

Lemma 5.2.4 (**Vinh**, [90]). *For any odd prime power q, $d \geq 1$, then $C_P(\mathbb{F}_q^{d+1})$ is an*

$$(q^{d+1}, q^d, q^{d/2}) - \textit{digraph.}$$

Let $P'(x_1, \ldots, x_{2d})$ be a polynomial in $\mathbb{F}_q[x_1, \ldots, x_{2d}]$ defined by $P' = P(x_1, \ldots, x_d) - P(x_{d+1}, \ldots, x_{2d})$. As a consequence of Lemma 5.2.4, we obtain the following lemma.

Lemma 5.2.5 (**Vinh**, [90]). *For any odd prime power q, $d \geq 1$, let $P'(x_1, \ldots, x_{2d})$ be a polynomial in $\mathbb{F}_q[x_1, \ldots, x_{2d}]$ defined by $P' = P(x_1, \ldots, x_d) - P(x_{d+1}, \ldots, x_{2d})$. Then $C_{P'}(\mathbb{F}_q^{2d+1})$ is an*

$$(q^{2d+1}, q^{2d}, q^d) - \textit{digraph.}$$

5.3 Proofs of Theorems 5.1.2 and 5.1.3

Proof of Theorem 5.1.2 We use the Cayley graph $C_P(\mathbb{F}_q^{d+1})$ to prove Theorem 5.1.2. Let $\mathscr{P} = \{(x_{i1}, \ldots, x_{id})\}_i$ be a set of n points in $\mathbb{F}_q^d$, and $S = \{(r_i, (y_{i1}, \ldots, y_{id}))\}_i$ a set of pairs of radii and centers representing P-spheres in $\mathscr{S}$. Let $U = \{(0, x_{i1}, \ldots, x_{id})\}_i \subset \mathbb{F}_q^{d+1}$ and $W = \{(r_i, y_{i1}, \ldots, y_{id})\}_i \subset \mathbb{F}_q^{d+1}$. Then the number of incidences between points and P-spheres is the number of edges between U and W in $C_P(\mathbb{F}_q^{d+1})$. Using Lemma 5.2.3 and 5.2.4, Theorem 5.1.2 follows.

Proof of Theorem 5.1.3 We use the sum-product graph $\mathscr{SP}(\mathbb{Z}_q^{d+1})$ to prove Theorem 5.1.3. We identify each point $(b_1, \ldots, b_d)$ in $\mathscr{P}$ with a vertex $(-b_1^2 - \cdots - b_d^2, b_1, \ldots, b_d) \in \mathbb{Z}_q^{d+1}$ of $\mathscr{SP}(\mathbb{Z}_q^{d+1})$, and each sphere $(x_1 - a_1)^2 + \cdots + (x_d - a_d)^2 = r$ in $\mathscr{S}$ with a vertex $(r - a_1^2 - \cdots - a_d^2, -2a_1, \ldots, -2a_d) \in \mathbb{Z}_q^{d+1}$ of $\mathscr{SP}(\mathbb{Z}_q^{d+1})$. Let $U \subset \mathbb{Z}_q^{d+1}$ be the set of points corresponding to $\mathscr{P}$, and $W \subset \mathbb{Z}_q^{d+1}$ the set of points corresponding to $\mathscr{S}$. Then the number of incidences between points and spheres is the number of edges between U and W in the sum-product graph $\mathscr{SP}(\mathbb{Z}_q^{d+1})$. By Lemma 5.2.1 and Lemma 5.2.2, Theorem 5.1.3 follows.

5.4 Generalized pinned distance problem

Proof of Theorem 5.1.4: First we prove that

$$\frac{1}{|\mathscr{E}|} \sum_{p \in \mathscr{E}} |\Delta_P(\mathscr{E}, p)| > (1 - c^2)q.$$

We identify each point $p = (b_1, \ldots, b_d) \in \mathscr{E}$ with a point $(0, b_1, \ldots, b_d) \in \mathbb{F}_q^{d+1}$, and each pair $(p = (b_1, \ldots, b_d), t)$ where $t \in \Delta_P(\mathscr{E}, p)$ with a point $(t, b_1, \ldots, b_d) \in \mathbb{F}_q^{d+1}$. Let $U \subset \mathbb{F}_q^{d+1}$ be the set of points corresponding to $\mathscr{E}$, and $W \subset \mathbb{F}_q^{d+1}$ the set of points corresponding to point-distance pairs. Then $|U| = |\mathscr{E}|$, $|W| = \sum_{p\in\mathscr{E}} |\Delta_P(\mathscr{E}, p)|$. Moreover, one can easily see that U, W are vertex subsets of the Cayley digraph $C_P(\mathbb{F}_q^{d+1})$. The number of edges between U and W is $|\mathscr{E}|^2$, since each point in $\mathscr{E}$ contributes $|\mathscr{E}|$ edges between U and W. It follows from Lemmas 5.2.3 and 5.2.4 that

$$\begin{aligned} |\mathscr{E}|^2 \le e(U,W) &\le \frac{|U||W|}{q} + q^{d/2}\sqrt{|U||W|}. \\ &= \frac{|\mathscr{E}|\sum_{p\in\mathscr{E}} |\Delta_P(\mathscr{E}, p)|}{q} + q^{d/2}\sqrt{|\mathscr{E}|\sum_{p\in\mathscr{E}} |\Delta_P(\mathscr{E}, p)|}. \end{aligned} \tag{5.4.1}$$

If $\frac{1}{|\mathscr{E}|}\sum_{p\in\mathscr{E}} |\Delta_P(\mathscr{E}, p)| \le (1-c^2)q$, it follows from (5.4.1) that

$$\begin{aligned} |\mathscr{E}|^2 &\le |\mathscr{E}|^2(1-c^2) + q^{(d+1)/2}|\mathscr{E}|\sqrt{(1-c^2)} \\ |\mathscr{E}| &\le \sqrt{\frac{(1-c^2)}{c^4}}q^{(d+1)/2}. \end{aligned}$$

This would be a contradiction. Therefore,

$$\sum_{p\in\mathscr{E}} |\Delta_P(\mathscr{E}, p)| > (1-c^2)q|\mathscr{E}|. \tag{5.4.2}$$

Let us define $\mathscr{E}' := \{p \in \mathscr{E} : |\Delta_Q(\mathscr{E}, p)| > (1-c)q\}$. Suppose that $|\mathscr{E}'| < (1-c)|\mathscr{E}|$, so

$$\sum_{p\in\mathscr{E}\setminus\mathscr{E}'} |\Delta_P(\mathscr{E}, p)| \le (|\mathscr{E}| - |\mathscr{E}'|)(1-c)q, \tag{5.4.3}$$

and

$$\sum_{p\in\mathscr{E}'} |\Delta_P(\mathscr{E}, p)| \le q|\mathscr{E}'|. \tag{5.4.4}$$

Putting (5.4.3) and (5.4.4) together, we obtain

$$\sum_{p\in\mathscr{E}} |\Delta_P(\mathscr{E}, p)| \le (1-c)q|\mathscr{E}| + cq|\mathscr{E}'| < (1-c)q|\mathscr{E}| + cq(1-c)|\mathscr{E}| = (1-c^2)q|\mathscr{E}|.$$

The theorem follows because this contradicts (5.4.2).

5.5 Related Problems

Incidences between random points and P-spheres: To prove Theorem 5.1.5, we need the following lemma (see [57, Lemma 8], and [91, Lemma 2.3] for more details).

Lemma 5.5.1. *Let $\{G_n = G(U_n, V_n)\}_{n=1}^{\infty}$ be a sequence of bipartite graphs with $|V_n| = |U_n| \to \infty$ as $n \to \infty$, and let $\bar{d}(G_n)$ be the average degree of G_n. Assume that for any $\varepsilon > 0$, there exists an integer $v(\varepsilon)$ and a number $c(\varepsilon) > 0$ such that*

$$e(A,B) \geq c(\varepsilon)|A||B|\frac{\bar{d}(G_n)}{|V_n|},$$

for all $|V_n| = |U_n| \geq v(\varepsilon)$ and all $A \subset V_n, B \subset U_n$ satisfying $|A||B| \geq \varepsilon|V_n|^2$. Then for any $\alpha > 0$, there exist an integer $v(\alpha)$ and a number $C(\alpha)$ with the following property: if one chooses a random subset S of V_n of cardinality t and a random subset T of U_n of the same cardinality t, then the probability of $G(S,T)$ being empty is at most α^t provided that $t \geq C(\alpha)|V_n|/\bar{d}(G_n)$ and $|V_n| \geq v(\alpha)$.

We notice that the Lemma 5.5.1 also holds when $\{G_n\}_n$ is a sequence of digraphs.

Proof of Theorem 5.1.5: Let $B_{q,d}$ be a bipartite digraph with vertex set $V(C_P(\mathbb{F}_q^{d+1})) \times V(C_P(\mathbb{F}_q^{d+1}))$, where $C_P(\mathbb{F}_q^{d+1})$ is the Cayley graph defined as in Lemma 5.2.4 and the edge set

$$\{\big((x_0,x),(y_0,y)\big) \in \mathbb{F}_q^{d+1} \times \mathbb{F}_q^{d+1} \mid (x_0 - y_0) + P(x-y) = 0\}.$$

With the same identification of the point set and the P-sphere set as in proof of Theorem 5.1.2, we obtain two corresponding sets U and W, where $|U| = |\mathscr{P}|$, $|W| = |\mathscr{S}|$. Thus, the number of incidences between points and spheres is the number of edges between U and W. By Lemma 5.2.3 and 5.2.4, we obtain

$$\left| e(U,W) - \frac{|U||W|}{q} \right| \leq q^{d/2}\sqrt{|U||W|}. \tag{5.5.1}$$

For any $\varepsilon > 0$ such that $|U||W| \geq \varepsilon q^{2d+2}$ and $q^d \geq \frac{4}{\varepsilon}$, we have from (5.5.1) that

$$e(U,W) \geq \frac{q^d}{2q^{d+1}}|U||W| = \frac{\bar{d}(B_{q,d})}{|V(B_{q,d})|}|U||W|.$$

Let $c(\varepsilon) = 1$, $v(\varepsilon) \geq (\frac{4}{\varepsilon})^{(d+1)/d}$, then the theorem follows from Lemma 5.5.1.

Generalized isosceles triangles:

Proof of Theorem 5.1.6: Let

$$U = \{(1, x, x) \in 1 \times \mathscr{E} \times \mathscr{E}\},\ W = \{(1, y, z) \in 1 \times \mathscr{E} \times \mathscr{E}\}.$$

One can easily see that $|U| = |\mathscr{E}|, |W| = |\mathscr{E}|^2$. Let

$$T_1 = \{(1, x, x, 1, y, z) \in 1 \times \mathscr{E} \times \mathscr{E} \times 1 \times \mathscr{E} \times \mathscr{E} : P(x-y) = P(x-z)\}.$$

Then the cardinality of T_1 is the number of edges between the sets U and W in the graph $C_{P'}(\mathbb{F}_q^{2d+1})$ (defined as in Lemma 5.2.5). It follows from Lemma 5.2.3 and 5.2.5 that

$$\left| |T_1| - \frac{|U||W|}{q} \right| \leq q^d \sqrt{|U||W|}.$$

Thus, if $|\mathscr{E}| \gg q^{2(d+1)/3}$ then $|T_1| = (1 + o(1))|\mathscr{E}|^3/q$. We notice that T_1 also contains the tuples $(1, x, x, 1, x, y)$ with $P(x-y) = 0$ which correspond to the edges between the vertices $(1, x, x) \in U$ and $(1, x, y) \in W$. Let us denote the set of such tuples by T_{err}, then one can easily see that $\frac{1}{2}|T_{err}|$ is the number of pairs $(x, y) \in \mathscr{E} \times \mathscr{E}$ such that $P(x-y) = 0$, since each pair (x, y) with $P(x-y) = 0$ contributes two edges $((1, x, x), (1, x, y))$ and $((1, x, x), (1, y, x))$. It follows from Lemma 5.2.3 and 5.2.4 that

$$\left| |T_{err}| - \frac{|\mathscr{E}|^2}{q} \right| \leq q^{d/2} \sqrt{|\mathscr{E}|^2}.$$

Thus, if $|\mathscr{E}| \gg q^{2(d+1)/3}$ with $d \geq 2$, then $|T_{err}| = |\mathscr{E}|^2/q = o(1)|\mathscr{E}|^3/q$. Therefore, the number of P-isosceles triangles determined by $\mathscr{E}$ is $(1 + o(1))|\mathscr{E}|^3/q$.

Distinct distances subset: In order to prove Theorem 5.1.7, we need the following theorem on the cardinality of a maximal independent set of a hypergraph due to Spencer [75].

Theorem 5.5.2. *Let H be a k-uniform hypergraph with n vertices and $m \geq n/k$ edges, and let $\alpha(H)$ denote the independence number of H. Then*

$$\alpha(H) \geq \left(1 - \frac{1}{k}\right) \left\lfloor \left(\frac{1}{k} \frac{n^k}{m}\right)^{\frac{1}{k-1}} \right\rfloor.$$

Proof of Theorem 5.1.7: Let

$$T_2 = \{(1, p_1, q_1, 1, p_2, q_2) \in 1 \times \mathscr{E} \times \mathscr{E} \times 1 \times \mathscr{E} \times \mathscr{E} : P(p_1 - q_1) = P(p_2 - q_2)\}.$$

With the same arguments in the proof of Theorem 5.1.6, we obtain $|T_2| \le \frac{|\mathscr{E}|^4}{q} + q^d|\mathscr{E}|^2$. Thus, if $|\mathscr{E}| \gg q^{(d+1)/2}$, then

$$|T_2| = (1+o(1))\frac{|\mathscr{E}|^4}{q}.$$

A 4-tuple of distinct elements in $\mathscr{E}^4$ is called *regular* if all six generalized distances determined are distinct. Otherwise, it is called *singular*. Let H be the 4-uniform hypergraph on the vertex set $V(H) = \mathscr{E}$, whose edges are the singular 4-tuples of $\mathscr{E}$.

It follows from Theorem 5.1.6 that the number of 4-tuples containing a triple induced an isosceles triangle is at most $((1+o(1))|\mathscr{E}|^3/q) \cdot |\mathscr{E}| = (1+o(1))|\mathscr{E}|^4/q$ when $|\mathscr{E}| \gg q^{2(d+1)/3}$. Thus the number of edges of H containing a triple induced an isosceles triangle is at most $(1+o(1))|\mathscr{E}|^4/q$. On the other hand, since $T_2 = (1+o(1))|\mathscr{E}|^4/q$ when $|\mathscr{E}| \gg q^{(d+1)/2}$, the number of 4-tuples (p_1, q_1, p_2, q_2) in $\mathscr{E}^4$ satisfying $P(p_1 - q_1) = P(p_2 - q_2)$ equals $(1+o(1))|\mathscr{E}|^4/q$ when $|\mathscr{E}| \gg q^{(d+1)/2}$. Thus, if $|\mathscr{E}| \gg q^{2(d+1)/3}$ with $d \ge 2$, then

$$|E(H)| \le \frac{2|\mathscr{E}|^4}{q}.$$

It follows from Theorem 5.5.2 that

$$\alpha(H) \ge C\left(\frac{|\mathscr{E}|^4}{|E(H)|}\right)^{1/3} = Cq^{1/3},$$

for some positive constant C. Since there is no repeated generalized distance determined by the independent set of H, we have $|U_Q| \ge \alpha(H) \ge Cq^{1/3}$.

Moreover, it is easy to see that there is at least one repeated generalized distance determined by any set of $\sqrt{2}q^{1/2}+1$ elements since there are only $q = |\mathbb{F}_q|$ distances over $\mathbb{F}_q^d$. Thus, the theorem follows.

6 Distinct spreads in finite spaces

6.1 Introduction

Let $q = p^r$ be a large odd prime power, and $\mathbb{F}_q$ be a finite field of order q. For three points $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}_q^d$, the spread between two vectors $\overrightarrow{\mathbf{ab}}$ and $\overrightarrow{\mathbf{ac}}$ in $\mathbb{F}_q^d$, which is denoted by $S(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}})$ (or $S(\mathbf{b}, \mathbf{a}, \mathbf{c})$ for simplicity), is defined as

$$S\left(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}}\right) := 1 - \frac{\left(\overrightarrow{\mathbf{ab}} \cdot \overrightarrow{\mathbf{ac}}\right)^2}{\|\overrightarrow{\mathbf{ab}}\| \cdot \|\overrightarrow{\mathbf{ac}}\|},$$

where $\|\overrightarrow{\mathbf{x}}\| = x_1^2 + \cdots + x_d^2$. If either term in the denominator is 0, then $S(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}})$ is undefined.

It is clear that this definition is consistent with the square of the sine of the angle between two vectors $\overrightarrow{\mathbf{ab}}$ and $\overrightarrow{\mathbf{ac}}$ in Euclidean space

$$\sin(\theta)^2 = 1 - \frac{\left(\overrightarrow{\mathbf{ab}} \cdot \overrightarrow{\mathbf{ac}}\right)^2}{\|\overrightarrow{\mathbf{ab}}\| \cdot \|\overrightarrow{\mathbf{ac}}\|}.$$

The following are some properties of the spread between two vectors $\overrightarrow{\mathbf{ab}}$ and $\overrightarrow{\mathbf{ac}}$:

(i) $S\left(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}}\right) = S\left(r(\overrightarrow{\mathbf{ab}}), s(\overrightarrow{\mathbf{ab}})\right)$ for any $r, s \in \mathbb{F}_q^*$,

(ii) $S\left(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}}\right) = S\left(\overrightarrow{\mathbf{ac}}, \overrightarrow{\mathbf{ab}}\right)$,

(iii) $S\left(\overrightarrow{\mathbf{ab}}, \overrightarrow{\mathbf{ac}}\right) = S\left(M \cdot \overrightarrow{\mathbf{ab}}, M \cdot \overrightarrow{\mathbf{ac}}\right)$, where M is an orthogonal matrix.

In 2015, Bennett [4] made the first investigation on the number of distinct spreads determined by points in $\mathscr{P} \subseteq \mathbb{F}_q^d$. In particular, he obtained the following.

Theorem 6.1.1 (Theorem 6.5, [4]). *Let $\mathscr{P}$ be a set of points in $\mathbb{F}_q^2$. If $|\mathscr{P}| \geq 2q-1$ then the number of distinct spreads generated by points in $\mathscr{P}$ is q.*

It is clear that Theorem 6.1.1 is sharp up to the coefficient of q, since the number of spreads spanned by points in a line of q points is at most one. For higher dimensional cases, Bennett [4] had an observation on a connection between spreads and distances:

A connection between spreads and distances on a sphere: Suppose $\mathscr{P}_1$ is a subset in the unit sphere S_1, it is easily to check that $S\left(\overrightarrow{\mathbf{0a}}, \overrightarrow{\mathbf{0b}}\right) = S\left(\overrightarrow{\mathbf{0c}}, \overrightarrow{\mathbf{0d}}\right)$ with $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathscr{P}_1$ if and only if either $\|\mathbf{a}-\mathbf{b}\| = \|\mathbf{c}-\mathbf{d}\|$ or $\|\mathbf{a}-\mathbf{b}\| = \|\mathbf{c}+\mathbf{d}\|$. Thus if $\mathscr{P}_1$ determines a positive proportion of all distances then $\mathscr{P}_1$ generates a positive proportion of all spreads. Therefore if we have a set $\mathscr{P} \subset \mathbb{F}_q^d$ satisfying $|\mathscr{P}| \gg q^{\frac{d+2}{2}}$ then there exists a sphere of radius $t \neq 0$ such that $|S_t \cap \mathscr{P}| \gg q^{d/2}$. From the first property of spread, we may assume that S_t is the unit sphere. It follows from Theorem 6.2.1 below that $S_1 \cap \mathscr{P}$ determines a positive proportion of all distances, therefore $S_1 \cap \mathscr{P}$ generates a positive proportion of all spreads. In other words, we have proved the following.

Theorem 6.1.2 (Theorem 6.3, [4]). *Let $\mathscr{P}$ be a set of points in $\mathbb{F}_q^d$, with $d \geq 3$. If $|\mathscr{P}| \gg q^{(d+2)/2}$ then $\mathscr{P}$ generates a positive proportion of all spreads.*

We remark here that if $\mathscr{P}$ is a subset in the unit sphere S_1, Vinh [88] showed that for $\mathscr{P} \subseteq \mathbb{F}_q^3$ with $|\mathscr{P}| \gg q^{3/2}$, the number of occurrences of a fixed spread γ among $\mathscr{P}$ is $\Theta\left(\frac{|\mathscr{P}|^2}{q}\right)$ if $1-\gamma$ is not a square in $\mathbb{F}_q$.

The main purpose of this chapter is to give sharp results on the number of distinct spreads generated by a large set in $\mathbb{F}_q^d$. Our first result gives us the number of distinct spreads generated by $\mathscr{P} \subseteq \mathbb{F}_q^d$ with d even.

Theorem 6.1.3. *For any $\varepsilon > 0$, there exists $c > 0$ such that the following holds. Let $\mathscr{P}$ be a set of points in $\mathbb{F}_q^d$ with $d \geq 2$ even. If $|\mathscr{P}| \geq (1+\varepsilon)q^{d/2}$, then the number of distinct spreads determined by $\mathscr{P}$ is at least cq.*

If $\mathscr{P}$ be a subset in $\mathbb{F}_q^d$ with d odd, then we can embed $\mathscr{P}$ in $\mathbb{F}_q^{d+1}$ with the last coordinate of 0. Therefore, as a direct consequence of Theorem 6.1.3, we obtain the following result.

Theorem 6.1.4. *For any $\varepsilon > 0$, there exists $c > 0$ such that the following holds. Let $\mathscr{P}$ be a set of points in $\mathbb{F}_q^d$ with $d \geq 3$ odd. If $|\mathscr{P}| \geq (1+\varepsilon)q^{(d+1)/2}$, then the number of distinct spreads determined by $\mathscr{P}$ is at least cq.*

We now show that the conditions on the size of $\mathscr{P}$ in Theorem 6.1.3 and Theorem 6.1.4 are sharp.

Theorem 6.1.5. *Let $\mathbb{F}_q$ be a finite field of order q with $q \equiv 1 \mod 4$. Then there exists a subset $\mathscr{P}$ in $\mathbb{F}_q^d$ with $d \geq 4$ even such that $|\mathscr{P}| = q^{d/2}$ and there is no spread determined by points in $\mathscr{P}$.*

Theorem 6.1.6. *Let $\mathbb{F}_q$ be a finite field of order q with $q \equiv 1 \mod 4$. Then there exists a subset $\mathscr{P}$ in $\mathbb{F}_q^d$ with $d \geq 3$ odd such that $|\mathscr{P}| = q^{(d+1)/2}$ and the number of distinct spreads determined by points in $\mathscr{P}$ is at most one.*

6.2 Proof of Theorem 6.1.3

For the convenience, we recall the following theorem on the number of distinct distances on the unit sphere due to Hart et al. [35].

Theorem 6.2.1 (**Hart et al.**, [35])**.** *For $\mathscr{P} \subseteq S_1$ in $\mathbb{F}_q^d$ with $d \geq 3$. Suppose that $|\mathscr{P}| \geq Cq^{\frac{d}{2}}$ for some positive constant C, then the number of distinct distances determined by points in $\mathscr{P}$ is at least* $\min\{q/2, Cq/4\}$.

To prove Theorem 6.1.3, we make use of the following theorem due to Lund and Saraf in [53].

Theorem 6.2.2 (Corollary 5, [53])**.** *For any $\varepsilon > 0$ and $\mathscr{P} \subseteq \mathbb{F}_q^d$ with $|\mathscr{P}| \geq (1+\varepsilon)q^{d-1}$, the number of lines spanned by $\mathscr{P}$ is bounded below by $\alpha_\varepsilon q^{2d-2}$, where $\alpha_\varepsilon = \varepsilon^2(1+\varepsilon+\varepsilon^2)^{-1}$.*

By using Theorem 6.2.2, we are able to show in our following theorem that if the cardinality of $\mathscr{P}$ is much smaller than q^{d-1}, we still have many distinct lines spanned by $\mathscr{P}$.

Theorem 6.2.3. *For any $0 < \varepsilon < q-1$, let $\mathscr{P} \subseteq \mathbb{F}_q^d$ with $|\mathscr{P}| \geq (1+\varepsilon)q^{k-1}$. Then, the number of lines spanned by $\mathscr{P}$ is bounded below by $(1-o(1))\alpha_\varepsilon q^{2k-2}$.*

Proof. Assume that $(1+\varepsilon)|\mathscr{P}|$ is an integer, and remove all but exactly $(1+\varepsilon)|\mathscr{P}|$ points from $\mathscr{P}$. Error introduced by assuming that $(1+\varepsilon)|\mathscr{P}|$ is an integer will only affect the $o(1)$ term in the result, and removing points from $\mathscr{P}$ only decreases the number of lines spanned by $\mathscr{P}$.

Let π' be a uniformly random projection from $\mathbb{F}_q^d$ to $\mathbb{F}_q^k$.

Let $\mathbf{a}, \mathbf{b}$ be two arbitrary distinct points in $\mathbb{F}_q^d$. We claim that the probability that $\pi'(\mathbf{a}) = \pi'(\mathbf{b})$ is less than q^{-k}. Note that, if $\pi'(\mathbf{a}) = \pi'(\mathbf{b})$, then $\pi'(\mathbf{a}-\mathbf{x}) = \pi'(\mathbf{b}-\mathbf{x})$ for

an arbitrary translation vector $\mathbf{x}$. Hence, we may without loss of generality assume that $\mathbf{a} = \mathbf{0}$. Then, the quesiton of whether $\pi'(\mathbf{a}) = \pi'(\mathbf{b})$ reduces to the question of whether $\mathbf{b}$ lies in the kernel of π', which is a uniformly random $(d-k)$-dimensional linear subspace. This probability is $(q^{d-k}-1)/q^d < q^{-k}$.

Hence, by linearity of expectation, the expected number of pairs $\mathbf{a}, \mathbf{b} \in P$ such that $\pi'(\mathbf{a}) = \pi'(\mathbf{b})$, denoted by E_{coll}, is $E_{coll} < \binom{|\mathscr{P}|}{2} q^{-k} = (1-o(1))(1+\varepsilon)^2 q^{k-2}/2$. In particular, there exists a projection π from $\mathbb{F}_q^d$ to $\mathbb{F}_q^k$ such that the number of such collisions is at most E_{coll}. By a Bonferroni inequality, the image $\pi(\mathscr{P})$ of $\mathscr{P}$ has size at least $|\pi(\mathscr{P})| \geq |\mathscr{P}| - E_{coll}$. Thus $|\pi(\mathscr{P})| = (1-o(1))|\mathscr{P}|$. The conclusion of the theorem follows from Theorem 6.2.2, and the observation that $\pi(\mathscr{P})$ does not span more lines than $\mathscr{P}$. □

Corollary 6.2.4. *Let $\mathscr{P}$ be a set of points in $\mathbb{F}_q^d$ with d even, and $\mathscr{L}$ be the set of spanned lines by $\mathscr{P}$. Suppose that $|\mathscr{P}| = (1+\varepsilon)q^{d/2}$, $\varepsilon > 0$, then there exists a point $\mathbf{p}$ in $\mathscr{P}$ such that it is incident to at least $(1-o(1))\frac{\alpha_\varepsilon}{1+\varepsilon} q^{d/2}$ lines from $\mathscr{L}$.*

Proof. It follows from Theorem 6.2.3 that the number of lines spanned by $\mathscr{P}$ is bounded below by $(1-o(1))\alpha_\varepsilon q^d$. By the pigeonhole-principle, there exists a point $\mathbf{p}$ in $\mathscr{P}$ such that it is incident to at least $(1-o(1))\frac{\alpha_\varepsilon}{1+\varepsilon} q^{d/2}$ lines, and the corollary follows. □

Proof of Theorem 6.1.3: By Corollary 6.2.4, if $|\mathscr{P}| \geq (1+\varepsilon)q^{d/2}$, then there exists a point $\mathbf{p}$ in $\mathscr{P}$ such that it is incident to at least $cq^{d/2}$ lines that are spanned by $\mathscr{P}$ for some positive constant c depending on ε.

Suppose $d = 2$. Then, if $\sqrt{-1} \in \mathbb{F}_q$, then there are $q-1$ points of $\mathbb{F}_q^2$ at distance 0 from $\mathbf{p}$, lying on a single isotropic line with slope $\sqrt{-1}$. If $\sqrt{-1} \notin \mathbb{F}_q$, then there is no point distinct from $\mathbf{p}$ at zero distance from $\mathbf{p}$. If $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathscr{P}$ such are in three distinct, non-isotropic lines incident to $\mathbf{p}$, then an easy calculation shows that $S(\mathbf{a}, \mathbf{p}, \mathbf{b}) \neq S(\mathbf{a}, \mathbf{p}, \mathbf{c})$, which proves Theorem 6.1.3 in the case $d = 2$.

Suppose $d > 2$. We denote the set of lines incident to $\mathbf{p}$ by $\mathscr{L}'$. One can check that there exists a sphere S_t of radius $t \neq 0$ such that $|S_t \cap \mathscr{L}'| \geq \frac{cq^{d/2}}{2}$. Without loss of generality, we assume that $\mathbf{p} = \mathbf{0}$ and $t = 1$. Theorem 6.2.1 implies that $S_1 \cap \mathscr{L}'$ determines a positive proportion of all distances. Thus Theorem 6.1.3 follows from the connection between spreads and distances given in the introduction. □

6.3 Proofs of Theorems 6.1.5 and 6.1.6

In this section, we will use the construction given in [35, Lemma 5.1]. We denote $i = \sqrt{-1}$, which is guaranteed to exist since we assume that $q \equiv 1 \mod 4$.

Proof of Theorem 6.1.5: Suppose $d = 2m$ with $m \geq 2$. Let $\mathscr{P}$ be the subspace spanned by $\mathbf{v}_1, \ldots, \mathbf{v}_m$, where

$$\mathbf{v}_1 = (1, i, 0, \ldots, 0), \mathbf{v}_2 = (0, 0, 1, i, 0 \ldots, 0), \ldots, \mathbf{v}_m = (0, \ldots, 0, 1, i).$$

It is easy to check that all vectors $\mathbf{v}_i$ are null orthogonal, i.e. $\mathbf{v}_i \cdot \mathbf{v}_j = 0$ for all $1 \leq i, j \leq m$. Since $\|\mathbf{v}_i\| = 0$ for all $1 \leq i \leq m$, it follows from the definition of spread that there is no spread determined by three vectors in $\mathscr{P}$. On the other hand, the size of $\mathscr{P}$ is $q^{d/2}$, which ends the proof of the theorem. □

Proof of Theorem 6.1.6: Suppose $d = 2m+1$ with $m \geq 2$. Let $\mathscr{P}$ be the subspace spanned by $\mathbf{v}_1, \ldots, \mathbf{v}_{m+1}$, where

$$\mathbf{v}_1 = (1, i, 0, \ldots, 0), \mathbf{v}_2 = (0, 0, 1, i, 0 \ldots, 0), \ldots, \mathbf{v}_m = (0, \ldots, 0, 1, i, 0), \mathbf{v}_{m+1} = (0, \ldots, 0, 1).$$

We have the size of $\mathscr{P}$ is $q^{(d+1)/2}$. It is easy to check that the spread spanned by any triple of points in $\mathscr{P}$ is either undefined or one. Thus the number of distinct spreads spanned by $\mathscr{P}$ is at most one. This concludes the proof of the theorem. □

7 Paths in pseudo-random graphs and applications

7.1 Introduction

Let $G = G(n,p)$ be a random graph. For a fixed graph H with $s \le n$ vertices, r edges, and automorphism group $\mathtt{Aut}(H)$, it is well-known that the number of induced copies of H in G is

$$(1+o(1))\, p^r (1-p)^{\binom{s}{2}-r} \frac{n^s}{|\mathtt{Aut}(H)|}.$$

Let G be a graph, and $\gamma_1 \ge \gamma_2 \ge \ldots \ge \gamma_n$ be the eigenvalues of the adjacency matrix A_G. The second eigenvalue of G is defined as $\gamma(G) := \max\{\gamma_2, -\gamma_n\}$. We say that G is an (n,d,γ)-*graph* if the size of $V(G)$ is n, the degree of each vertex is d, and $\gamma(G)$ is bounded from above by γ. Noga Alon [49] established that the number of copies of any fixed graph in a large vertex set of an (n,d,γ)-graph is close to the expected value. In particular, the precise statement is as follows.

Theorem 7.1.1 (**Alon**, Theorem 4.10 [49])**.** *Let H be a fixed graph with r edges, s vertices, and maximum degree Δ, and let $G = (V,E)$ be an (n,d,γ)-graph where $d \le 0.9n$. Let $m < n$ satisfy $\gamma(n/d)^{\Delta} = o(m)$. Then, for every subset $U \subset V$ of cardinality m, the number of (not necessarily induced) copies of H in U is*

$$(1+o(1))\frac{|U|^s}{|\mathtt{Aut}(H)|}\left(\frac{d}{n}\right)^r.$$

Note that if one takes the ordering of vertex set into account in Theorem 7.1.1, then the number of copies of H in U is $(1+o(1))|U|^s (d/n)^r$. In the case H is a complete bipartite graph $K_{s,t}$, it has been shown by Vinh [93] that the conditions on d and γ in Theorem 7.1.1 can be improved. Before presenting that result, we first need to introduce the following notations. Let $G \times G = (V_1 \cup V_2, E(G \times G))$ be the bipartite graph with the

vertex sets V_1 and V_2, and the edge set $E(G\times G)$, which are defined as: $V_1 = V_2 = V(G)$, $(u,v)\in V_1\times V_2\in E(G\times G)$ if $(u,v)\in E(G)$. For any two subsets $U_1, U_2\subset V(G)$, we denote the induced bipartite subgraph of $G\times G$ on $U_1\times U_2$ by $G(U_1,U_2)$.

Theorem 7.1.2 (Theorem 2.2, [93])**.** *Let t and s be integers with $t\geq s$ and $t\geq 2$, and $G=(V,E)$ be an (n,d,γ)-graph. For $U_1,U_2\subset V$, suppose that*

$$|U_1||U_2|\geq \gamma^2(n/d)^{t+s},$$

then $G(U_1,U_2)$ contains

$$(1+o(1))\frac{|U_1|^s|U_2|^t}{s!t!}\left(\frac{d}{n}\right)^{st}$$

copies of $K_{s,t}$.

When either s or t is very small, one can also improve the bound in Theorem 7.1.2, for instance, in the case $s=2$ and $t\geq 1$, the author of [93] indicated that under the condition $|U_1||U_2|\geq\gamma^2(n/d)^{t+1}$, the induced subgraph $G(U_1,U_2)$ contains $(1+o(1))\frac{|U_1|^s|U_2|^t}{2!t!}\left(\frac{d}{n}\right)^{st}$ copies of $K_{2,t}$.

Suppose U is a set of vertices in an (n,d,γ)-graph G, and H is a path of length k. It follows from Theorem 7.1.1 that if $\gamma(n/d)^2=o(|U|)$, then the number of copies of H in U is

$$(1+o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k.$$

Our main purpose of this chapter is to give an asymptotically tight condition on the size of $U\subset V$ such that the number of paths of length k in U is close to the expected number for arbitrary $k\geq 1$. As applications, we obtain improvements and generalizations of results in [5]. Our first main result is as follows.

Theorem 7.1.3. *Let $G=(V,E)$ be an (n,d,γ)-graph. Suppose that $U\subseteq V$ with $\gamma\left(\frac{n}{d}\right)=o(|U|)$. For an integer $k\geq 1$, let $P_k(U)$ be the number of paths of length k in U, i. e.*

$$P_k(U)=\#\left\{(u_1,\ldots,u_{k+1})\in U^{k+1}:\ u_iu_{i+1}\in E(G),1\leq i\leq k\right\}.$$

Then we have

$$P_k(U)=(1+o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k.$$

On the sharpness of Theorem 7.1.3, we have the following.

Theorem 7.1.4. *There exist an (n,d,γ)-graph G and a set U of vertices with $|U|=c\gamma\left(\frac{n}{d}\right)$ for some $0<c<1$ such that $P_k(U)=0$ for arbitrary $k\geq 1$.*

We say that a path $(u_1,\dots,u_{k+1}) \in U^{k+1}$ of length k is non-overlapping if $u_i \neq u_j$ for all $i \neq j$. For a set U of vertices in an (n,d,γ)-graph G, let $D_k(U)$ be the number of non-overlapping paths of length k in U, i.e.

$$D_k(U) = \#\left\{(u_1,\dots,u_{k+1}) \in U^{k+1} \colon\ u_i u_{i+1} \in E(G), 1 \le i \le k,\ u_i \neq u_j, \forall\, i \neq j\right\}.$$

In the following theorem, we show that under similar conditions on the size of U, the number of non-overlapping paths of length k in U is $(1-o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k$.

Theorem 7.1.5. *Let $G=(V,E)$ be an (n,d,γ)-graph. Suppose that $U \subseteq V$ with $\gamma\left(\frac{n}{d}\right) = o(|U|)$ and $k\left(\frac{n}{d}\right) = o(|U|)$, then we have*

$$D_k(U) = (1-o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k.$$

Note that Theorems 7.1.4 and 7.1.5 could be presented in *multi-color variants*, which will be used for our later applications. Let G be a graph, we color its edges by a set of finite colors. The graph G is called an (n,d,γ)-*colored graph* if for each color, the corresponding subgraph of G is an $(n,(1+o(1))d,\gamma)$-graph. Our next results are multi-color variants of Theorem 7.1.3 and Theorem 7.1.5.

Theorem 7.1.6. *Suppose $G=(V,E)$ is an (n,d,γ)-colored graph. For a sequence $c=(c_1,\dots,c_k)$ of k colors, and $U \subseteq V$, we define*

$$P_k^c(U) := \#\left\{(u_1,\dots,u_{k+1}) \in U^{k+1} \colon\ \text{the edge } u_i u_{i+1} \text{ is colored by } c_i, 1 \le i \le k\right\}.$$

If U satisfies $\gamma\left(\frac{n}{d}\right) = o(|U|)$, then we have

$$P_k^c(U) = (1+o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k.$$

Theorem 7.1.7. *Suppose $G=(V,E)$ is an (n,d,γ)-colored graph. For a sequence $c=(c_1,\dots,c_k)$ of k colors, and $U \subseteq V$, we define*

$$D_k^c(U) := \#\left\{(u_1,\dots,u_{k+1}) \in P_k^c(U) \colon\ u_i \neq u_j\ \forall\, i \neq j\right\}.$$

If U satisfies $\gamma\left(\frac{n}{d}\right) = o(|U|)$ and $k\left(\frac{n}{d}\right) = o(|U|)$, then we have

$$D_k^c(U) = (1+o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k.$$

For the sake of simplicity of this chapter we are only presenting the proofs of Theorems 7.1.3 and 7.1.5, since those of Theorems 7.1.6 and 7.1.7 are almost identical.

Applications: Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d, d \geq 2$, and $k \geq 1$ be an integer. Let $t = (t_1, \ldots, t_k) \in \mathbb{F}_q^k$ with $t_i \neq 0$, $1 \leq i \leq k$, we define

$$P_k^t(\mathscr{E}) := |\{(p_1, \ldots, p_{k+1}) \in \mathscr{E} \times \cdots \times \mathscr{E} : ||p_i - p_{i+1}|| = t_i,\ 1 \leq i \leq k\}|$$

as the number of paths of length k in $\mathscr{E}$ with given distances $(t_1, \ldots, t_k) \in \mathbb{F}_q^k$. In the case $k = 1$, we have $P_1^t(\mathscr{E})$ is the number of pairs $(x, y) \in \mathscr{E}^2$ of distance t_1. In a recent work, Bennett, Chapman, Covert, Hart, Iosevich and Pakianathan [5], using Fourier analytic techniques, studied the magnitude of $P_k^t(\mathscr{E})$ for arbitrary $k \geq 1$ as follows.

Theorem 7.1.8 (**Bennett et al.,** [5])**.** *For $\mathscr{E} \subset \mathbb{F}_q^d$, $d \geq 2$ and an integer $k \geq 1$. Suppose that $\frac{2k}{\ln 2} q^{\frac{d+1}{2}} = o(|\mathscr{E}|)$ then we have*

$$P_k^t(\mathscr{E}) = (1 + o(1)) \frac{|\mathscr{E}|^{k+1}}{q^k}.$$

As a consequence of Theorem 7.1.8, the authors of [5] indicated that under the same condition as in Theorem 7.1.8, there exist *non-overlapping* paths of length k in $\mathscr{E}$ with arbitrary $k \geq 1$. The precise statement is as follows.

Theorem 7.1.9 (**Bennett et al.,** [5])**.** *Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d, d \geq 2$, and $k \geq 1$ be an integer. Let $t = (t_1, \ldots, t_k)$ with $t_i \neq 0$, $1 \leq i \leq k$, we define*

$$D_k^t(\mathscr{E}) := |\{(p_1, \ldots, p_{k+1}) \in \mathscr{E} \times \cdots \times \mathscr{E} : ||p_i - p_{i+1}|| = t_i,\ 1 \leq i \leq k, p_i \neq p_j, \forall\, i \neq j\}|.$$

Suppose that $|\mathscr{E}| \geq \frac{2k}{\ln 2} q^{\frac{d+1}{2}}$ then we have $D_k^t(\mathscr{E}) > 0$.

Note that in the case $k = 1$, Theorem 7.1.9 implies the main result in [44]. In this section, we will present some improvements and generalizations of Theorems 7.1.8 and 7.1.9.

The finite Euclidean distance graphs: Suppose Q is a non-degenerate quadratic form on $\mathbb{F}_q^d$, and $\lambda \in \mathbb{F}_q \setminus \{0\}$, the finite Euclidean distance graph $E_q(d, Q, \lambda)$ is defined as follows:

$$V(E_q(d, Q, \lambda)) = \mathbb{F}_q^d,\ \ E\big(E_q(d, Q, \lambda)\big) = \{(x, y) \in V \times V :\ Q(x - y) = \lambda.\}$$

The (n,d,γ)-form of $E_q(d,Q,\lambda)$ has been studied in [2, 50].

Theorem 7.1.10 ([2, 50])**.** *Suppose Q is a non-degenerate quadratic form on $\mathbb{F}_q^d$. For any $\lambda \in \mathbb{F}_q \setminus \{0\}$, the graph $E_q(d,Q,\lambda)$ is an*

$$\left(q^d, (1+o(1))q^{d-1}, 2q^{\frac{d-1}{2}}\right) - \textit{graph.}$$

Let G be a graph with $V(G) = \mathbb{F}_q^d$, and we color the edge between two vertices x and y by the color $\lambda \in \mathbb{F}_q \setminus \{0\}$ if $Q(x-y) = \lambda$. Theorem 7.1.10 implies that the graph G is an $(q^d, (1+o(1))q^{d-1}, 2q^{\frac{d-1}{2}})$-colored graph with $(q-1)$ colors. Thus as consequences of Theorems 7.1.6 and 7.1.7, we are able to improve Theorems 7.1.8 and 7.1.9 as follows.

Theorem 7.1.11. *Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d, d \geq 2$, and $k \geq 1$ be an integer. Let $t = (t_1, \ldots, t_k)$ with $t_i \neq 0$, $1 \leq i \leq k$, we define*

$$P_k^t(\mathscr{E}) := |\{(p_1, \ldots, p_{k+1}) \in \mathscr{E} \times \cdots \times \mathscr{E} : Q(p_i - p_{i+1}) = t_i,\ 1 \leq i \leq k\}|.$$

Suppose that $q^{\frac{d+1}{2}} = o(|\mathscr{E}|)$, then we have

$$P_k^t(\mathscr{E}) = (1+o(1))\frac{|\mathscr{E}|^{k+1}}{q^k}.$$

Theorem 7.1.12. *Let $\mathscr{E}$ be a set in $\mathbb{F}_q^d, d \geq 2$, and $k \geq 1$ be an integer. Let $t = (t_1, \ldots, t_k)$ with $t_i \neq 0$, $1 \leq i \leq k$, we define*

$$D_k^t(\mathscr{E}) := |\{(p_1, \ldots, p_{k+1}) \in \mathscr{E} \times \cdots \times \mathscr{E} : Q(p_i - p_{i+1}) = t_i,\ 1 \leq i \leq k, p_i \neq p_j, \forall\, i \neq j\}|.$$

Suppose that $kq = o(|\mathscr{E}|)$ and $q^{\frac{d+1}{2}} = o(|\mathscr{E}|)$, then we have

$$D_k^t(\mathscr{E}) = (1+o(1))\frac{|\mathscr{E}|^{k+1}}{q^k}.$$

The finite upper half-plane graphs: For a finite field $\mathbb{F}_q$, the upper half plane, which is denoted by H_q, is defined as

$$H_q := \{z = x + y\sqrt{\sigma} : x, y \in \mathbb{F}_q \text{ and } y \neq 0\}, \tag{7.1.1}$$

where σ is a non-square in $\mathbb{F}_q$. For any two points $z = u + v\sqrt{\sigma}$ and $w = x + y\sqrt{\sigma}$ in H_q, the distance between two points is defined by

$$d(z,w) := \frac{(u-x)^2 - \sigma(v-y)^2}{vy}.$$

Although this distance function is not a metric, it has a property which is the same as the Euclidean distance function, namely it is $GL(2,\mathbb{F}_q)$-invariant: $d(gz,gw) = d(z,w)$ for all $g \in GL(2,\mathbb{F}_q)$ and all $z,w \in H_q$.

For $\lambda \in \mathbb{F}_q \setminus \{0,4\sigma\}$, the finite upper half-plane graph $P(\sigma,\lambda)$ is defined by: $V(P(\sigma,\lambda)) = H_q$ and $(z,w) \in E(P(\sigma,\lambda))$ if $d(z,w) = \lambda$. The (n,d,γ)-form of $P(\sigma,\lambda)$ has been established by Terras in [81].

Theorem 7.1.13 ([81])**.** *Let λ be an element in $\mathbb{F}_q \setminus \{0,4\sigma\}$, the finite upper half-plane graph $P(\sigma,\lambda)$ is*

$$\left(q^2-q, q+1, 2q^{1/2}\right) - \textit{graph.}$$

Let G be a graph with $V(G) = \mathbb{F}_q^d$, and we color the edge between two vertices z and w by the color $\lambda \in \mathbb{F}_q \setminus \{0,4\sigma\}$ if $d(z,w) = a$. Theorem 7.1.13 implies that the graph G is an $(q^2-q, q+1, 2q^{1/2})$-colored graph with $(q-2)$ colors. Therefore, as a consequence of Theorem 7.1.6, we have the following result.

Theorem 7.1.14. *Let $\mathscr{E}$ be a set in H_q, and $k \geq 1$ be an integer. Let $t = (t_1,\ldots,t_k)$ with $t_i \neq 0$, $1 \leq i \leq k$, we define*

$$P_k^t(\mathscr{E}) := |\{(p_1,\ldots,p_{k+1}) \in \mathscr{E} \times \cdots \times \mathscr{E} : d(p_i,p_{i+1}) = t_i,\ 1 \leq i \leq k\}|.$$

Suppose that $q^{\frac{3}{2}} = o(|\mathscr{E}|)$, then we have

$$P_k^t(\mathscr{E}) = (1+o(1))\frac{|\mathscr{E}|^{k+1}}{q^k}.$$

7.2 Proofs of Theorems 7.1.3–7.1.5

To prove Theorems 7.1.3–7.1.5, we will use the following lemmas.

Lemma 7.2.1 ([32])**.** *Let $G = (V,E)$ be an (n,d,γ)-graph. The number of edges between two multi-sets of vertices B and C in G satisfies:*

$$\left| e_m(B,C) - \frac{d|B||C|}{n} \right| \leq \gamma \sqrt{\sum_{b \in B} m_B(b)^2} \sqrt{\sum_{c \in C} m_C(c)^2},$$

where $m_X(x)$ is the multiplicity of x in X.

As a consequence of Lemma 7.2.1, we obtain the following recurrence relation between paths in U.

Lemma 7.2.2. *Let G be an (n,d,γ)-graph. For a subset U of vertices, let $P_k(U)$ be the number of paths of length k with vertices in U. Then we have the following*

$$\left|P_{2k+1}(U)-\frac{dP_k(U)^2}{n}\right|\le\gamma P_{2k}(U),\quad \left|P_{2k}(U)-\frac{dP_k(U)P_{k-1}(U)}{n}\right|\le\gamma\sqrt{P_{2k}(U)P_{2k-2}(U)}.$$

Proof. Let B and C be multi-sets defined as follows:

$$B:=\{u_{k+1}\colon (u_1,\dots,u_{k+1}) \text{ is a path of length } k \text{ in } U\},$$

$$C:=\{v_{k+2}\colon (v_{k+2},\dots,v_{2k+2}) \text{ is a path of length } k \text{ in } U\}.$$

One can check that P_{2k+1} is equal to the number of edges between B and C in the graph G. Thus it follows from Lemma 7.2.1 that

$$\left|P_{2k+1}(U)-\frac{dP_k(U)^2}{n}\right|\le\gamma\sqrt{\sum_{b\in B}m_B(b)^2}\sqrt{\sum_{c\in C}m_C(c)^2}.$$

It is easy to see that $\sum_{b\in B}m_B(b)^2=\sum_{c\in C}m_C(c)^2=P_{2k}(U)$. This implies that

$$\left|P_{2k+1}(U)-\frac{dP_k(U)^2}{n}\right|\le\gamma P_{2k}(U).$$

By using the same arguments, we obtain

$$\left|P_{2k}(U)-\frac{dP_k(U)P_{k-1}(U)}{n}\right|\le\gamma\sqrt{P_{2k}(U)P_{2k-2}(U)},$$

which completes the proof of the lemma. □

We will prove Theorem 7.1.3 by using induction on k, so we need the following theorems for the base cases $k=1$ and $k=2$.

Theorem 7.2.3. *Let $G=(V,E)$ be an (n,d,γ)-graph. Suppose that $U\subseteq V$ with $\gamma\left(\frac{n}{d}\right)=o(|U|)$, then the number of paths of length one in U is $(1+o(1))|U|^2\frac{d}{n}$.*

Proof. The number of paths of length one is the number of edges between U and U in G. Thus the theorem follows directly from Lemma 7.2.1. □

Theorem 7.2.4 (Theorem 3.3, [83])**.** *Suppose $G=(V,E)$ is an (n,d,γ)-graph. For $U\subseteq V$ with $\gamma\left(\frac{n}{d}\right)=o(|U|)$, we have that the number of paths of length two in U is $(1+o(1))|U|^3\left(\frac{d}{n}\right)^2$.*

We are now ready to prove Theorem 7.1.3.

Proof of Theorem 7.1.3. We first prove the upper bound of Theorem 7.1.3 by induction on k. The base cases $k = 1$ and $k = 2$ follow from Theorems 7.2.3 and 7.2.4. Suppose that the statement holds for all $2k \geq 1$. We now show that it also holds for $2k+1$ and $2k+2$. Indeed, it follows from Lemma 7.2.2 and induction hypothesis that

$$\begin{aligned} P_{2k+1}(U) \leq \frac{d}{n} P_k(U)^2 + \gamma P_{2k}(U) &\leq (1+o(1)) \left(\frac{d}{n}\right)^{2k+1} |U|^{2k+2} + (1+o(1))\gamma \left(\frac{d}{n}\right)^{2k} |U|^{2k+1} \\ &= (1+o(1)) \left(\frac{d}{n}\right)^{2k+1} |U|^{2k+2}, \end{aligned}$$

when $\gamma\left(\frac{n}{d}\right) = o(|U|)$.

For the case $2k+2$, it also follows from Lemma 7.2.2 that

$$P_{2k+2}(U) \leq \frac{dP_k(U)P_{k+1}(U)}{n} + \gamma\sqrt{P_{2k}(U)P_{2k+2}(U)}.$$

Solving this inequality in $x = \sqrt{P_{2k+2}}$, we obtain

$$P_{2k+2}(U) \leq \left(\gamma\sqrt{P_{2k}(U)} + \left(\frac{dP_k(U)P_{k+1}(U)}{n}\right)^{1/2}\right)^2.$$

By using the induction hypothesis, we have

$$P_{2k+2}(U) \leq (1+o(1)) \left(\frac{d}{n}\right)^{2k+2} |U|^{2k+3}.$$

In other words, we have proved that for all $k \geq 1$ and $\gamma\left(\frac{n}{d}\right) = o(|U|)$

$$P_k(U) \leq (1+o(1))|U|^{k+1} \left(\frac{d}{n}\right)^k.$$

By using the lower bounds of Lemma 7.2.2 and a nearly identical argument, we also obtain

$$P_k(U) \geq (1-o(1))|U|^{k+1} \left(\frac{d}{n}\right)^k,$$

under the condition $\gamma\left(\frac{n}{d}\right) = o(|U|)$. This completes the proof of the theorem. □

Proof of Theorem 7.1.4. Let $d \geq 3$ be an odd integer. From Theorem 7.1.10 we have

that for any $\lambda \in \mathbb{F}_q^*$, the graph $E_q(d,Q,\lambda)$ is an

$$\left(q^d, (1+o(1))q^{d-1}, 2q^{(d-1)/2}\right) - \text{graph}.$$

Suppose $Q(x) = x_1^2 + \cdots + x_d^2$. It has been shown in [35, Theorem 2.7] that there exist a set $U \subset \mathbb{F}_q^d$ with $|U| = cq^{(d+1)/2} = c\gamma\frac{n}{d}$ for some constant $0 < c < 1$ and $\beta \in \mathbb{F}_q^*$ such that there are no two points in U of distance β. This implies that there is no path of length k with arbitrary $k > 1$ in U in the graph $E_q(d,Q,\beta)$. □

In the proof of Theorem 7.1.5, we will use ideas given in [5, Corollary 1.3].

Proof of Theorem 7.1.5. Since the upper bound of Theorem 7.1.5 follows from Theorem 7.1.3, it suffices to prove that

$$D_k(U) \geq (1-o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k. \tag{7.2.1}$$

For $u \in U$, let $f_k(u)$ be the number of non-overlapping paths of length k in U beginning at $u \in U$. Then we have

$$D_k(U) = \sum_{u\in U} f_k(u).$$

We now prove (7.2.1) by induction on k. The base case $k = 1$ follows directly from Lemma 7.2.1. Suppose that the statement is true for all $k-1 \geq 1$, we now show that it also holds for k. Indeed, one can check easily that

$$D_{k+1}(U) \geq \sum_{u\in U} f_k(u)\,(d_U(u)-k) = -kD_k(U) + \sum_{u\in U} f_k(u)d_U(u). \tag{7.2.2}$$

On the other hand, by using the same arguments as in the proof of Lemma 7.2.2, we have

$$\left|\sum_{u\in U} f_k(u)d_U(u) - \frac{dD_k(U)|U|}{n}\right| \leq \gamma|U|^{1/2}\sqrt{\sum_{u\in U} f_k(u)^2} \leq \gamma|U|^{1/2}\sqrt{P_{2k}(U)},$$

where we use the estimate $\sum_{u\in U} f_k(u)^2 \leq P_{2k}(U)$. This implies that

$$\sum_{u\in U} f_k(u)d_U(u) \geq \frac{dD_k(U)|U|}{n} - \gamma|U|^{1/2}\sqrt{P_{2k}(U)} \geq \frac{dD_k(U)|U|}{n} - \gamma(1+o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k. \tag{7.2.3}$$

Putting (7.2.2) and (7.2.3) together gives us

$$D_{k+1}(U) \geq \frac{D_k(U)|U|d}{n} - kD_k(U) - \gamma(1+o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k.$$

By using the induction hypothesis and the conditions $\gamma\left(\frac{n}{d}\right) = o(|U|)$ and $k\left(\frac{n}{d}\right) = o(|U|)$, we obtain

$$D_{k+1}(U) \geq (1-o(1))|U|^{k+1}\left(\frac{d}{n}\right)^k,$$

which completes the proof of the theorem. □

7.3 Concluding remarks

We conclude this chapter with some remarks. Let $E_q(d,Q,\lambda)$ be the finite Euclidean distance graph defined in the introduction. It follows from Theorem 7.1.1 that for $\mathscr{E} \subset \mathbb{F}_q^d$, if $q^{\frac{d+3}{2}} = o(|\mathscr{E}|)$ then $\mathscr{E}$ contains many copies of a fixed triangle. Note that Theorem 7.1.1 can also be stated for (n,d,γ)-colored graphs, and in this form we have that the number of congruence classes of triangles in $\mathscr{E}$ is $(1-o(1))q^3$ under the condition $q^{\frac{d+3}{2}} = o(|\mathscr{E}|)$. However, this condition is only non-trivial when $d \geq 4$. If one can prove that under the same condition as in Theorem 7.1.3, i.e. $\gamma(n/d) = o(|\mathscr{E}|)$, $\mathscr{E}$ contains many copies of a fixed triangle, then this will imply that in the case $d = 2$, we only need the condition $q^{3/2} = o(|\mathscr{E}|)$ to get almost all of congruence classes of triangles, which matches Iosevich's conjecture [43] and the construction in [6]. Thus we are led to the following conjecture.

Conjecture 7.3.1. *Suppose $G = (V,E)$ is an (n,d,γ) graph. For $U \subseteq V$ with $\gamma\left(\frac{n}{d}\right) = o(|U|)$, we have that the number of copies of a fixed cycle C of length 3 in U is $(1+o(1))|U|^3\left(\frac{d}{n}\right)^3$.*

8 Sum-product estimates over arbitrary fields

8.1 Introduction

Let $\mathbb{F}$ be an arbitrary field. We use the convention that if $\mathbb{F}$ has positive characteristic, we denote the characteristic by p, while if $\mathbb{F}$ has characteristic zero, we set $p = \infty$. Thus, a condition like $N < p^{5/8}$ is restrictive in positive characteristic, but vacuous in characteristic zero. We denote the set of non-zero elements in $\mathbb{F}$ by $\mathbb{F}^*$.

For $\mathscr{A} \subset \mathbb{F}$, the sum and the product sets are defined as follows:

$$\mathscr{A} + \mathscr{A} = \{a + a' : a, a' \in \mathscr{A}\},\ \mathscr{A} \cdot \mathscr{A} = \{a \cdot a' : a, a' \in \mathscr{A}\}.$$

For $\mathscr{A} \subset \mathbb{F}_p$, Bourgain, Katz and Tao ([9]) proved that if $p^\delta < |\mathscr{A}| < p^{1-\delta}$ for some $\delta > 0$, then we have

$$\max\{|\mathscr{A} + \mathscr{A}|, |\mathscr{A} \cdot \mathscr{A}|\} \gg |\mathscr{A}|^{1+\varepsilon},$$

for some $\varepsilon = \varepsilon(\delta) > 0$.

In a breakthrough paper [64], Roche-Newton, Rudnev, and Shkredov improved and generalized this result to arbitrary fields. More precisely, they showed that for $\mathscr{A} \subset \mathbb{F}$, the sum set and the product set satisfy

$$\max\{|\mathscr{A} \pm \mathscr{A}|, |\mathscr{A} \cdot \mathscr{A}|\} \gg |\mathscr{A}|^{6/5},\ \max\{|\mathscr{A} \pm \mathscr{A}|, |\mathscr{A} : \mathscr{A}|\} \gg |\mathscr{A}|^{6/5}.$$

Note that the same bound also holds for $|\mathscr{A} + \mathscr{A}^2|$, $\max\left\{|\mathscr{A} + \mathscr{A}|, |\mathscr{A}^2 + \mathscr{A}^2|\right\}$ [61], and $|\mathscr{A}(1 + \mathscr{A})|$ [76]. We refer the reader to [1, 11, 64, 56] and references therein for recent results on the sum-product topic.

Let G be a subgroup of $\mathbb{F}^*$, and $g\colon G \to \mathbb{F}^*$ be an arbitrary function. We define

$$\mu(g) := \max_{t\in\mathbb{F}^*} \big|\{x \in G\colon g(x) = t\}\big|.$$

For $\mathscr{A}, \mathscr{B} \subset \mathbb{F}_p$ and two-variable functions $f(x,y)$ and $g(x,y)$ in $\mathbb{F}_p[x,y]$, Hegyvári and Hennecart [39], using graph theoretic techniques, proved that if $|\mathscr{A}| = |\mathscr{B}| = p^\alpha$, then

$$\max\big\{|f(\mathscr{A},\mathscr{B})|, |g(\mathscr{A},\mathscr{B})|\big\} \gg |\mathscr{A}|^{1+\Delta(\alpha)},$$

for some $\Delta(\alpha) > 0$. More precisely, they established the following results.

Theorem 8.1.1 (**Hegyvári and Hennecart**, [39]). *Let G be a subgroup of $\mathbb{F}_p^*$. Consider the function $f(x,y) = g(x)(h(x)+y)$ on $G \times \mathbb{F}_p^*$, where $g, h\colon G \to \mathbb{F}_p^*$ are arbitrary functions. Define $m = \mu(g\cdot h)$. For any subsets $\mathscr{A} \subset G$ and $\mathscr{B}, \mathscr{C} \subset \mathbb{F}_p^*$, we have*

$$\big|f(\mathscr{A},\mathscr{B})\big|\,|\mathscr{B}\cdot\mathscr{C}| \gg \min\left\{\frac{|\mathscr{A}||\mathscr{B}|^2|\mathscr{C}|}{pm^2}, \frac{p|\mathscr{B}|}{m}\right\}.$$

Theorem 8.1.2 (**Hegyvári and Hennecart**, [39]). *Let G be a subgroup of $\mathbb{F}_p^*$. Consider the function $f(x,y) = g(x)(h(x)+y)$ on $G \times \mathbb{F}_p^*$, where $g, h\colon G \to \mathbb{F}_p^*$ are arbitrary functions. Define $m = \mu(g)$. For any subsets $\mathscr{A} \subset G$, $\mathscr{B}, \mathscr{C} \subset \mathbb{F}_p^*$, we have*

$$|f(\mathscr{A},\mathscr{B})|\,|\mathscr{B}+\mathscr{C}| \gg \min\left\{\frac{|\mathscr{A}||\mathscr{B}|^2|\mathscr{C}|}{pm^2}, \frac{p|\mathscr{B}|}{m}\right\}.$$

It is worth noting that Theorem 6 established by Bukh and Tsimerman [11] does not cover such a function defined in Theorem 8.1.2. The reader can also find the generalizations of Theorems 8.1.1 and 8.1.2 in the setting of finite valuation rings in [31].

Suppose $f(x,y) = g(x)(h(x)+y)$ with $\mu(g), \mu(h) = O(1)$ and $\mathscr{A} = \mathscr{B} = \mathscr{C}$. Then, it follows from Theorems 8.1.1 and 8.1.2 that

1. If $|\mathscr{A}| \gg p^{2/3}$, then we have

$$|f(\mathscr{A},\mathscr{A})|\,|\mathscr{A}\cdot\mathscr{A}|, |f(\mathscr{A},\mathscr{A})|\,|\mathscr{A}+\mathscr{A}| \gg p|\mathscr{A}|.$$

2. If $|\mathscr{A}| \ll p^{2/3}$, then we have

$$|f(\mathscr{A},\mathscr{A})|\,|\mathscr{A}\cdot\mathscr{A}|, |f(\mathscr{A},\mathscr{A})|\,|\mathscr{A}+\mathscr{A}| \gg |\mathscr{A}|^4/p. \tag{8.1.1}$$

The main goal of this chapter is to improve and generalize Theorems 8.1.1 and 8.1.2 to arbitrary fields for small sets. Our first result is an improvement of Theorem 8.1.1.

Theorem 8.1.3. *Let $f(x,y) = g(x)(h(x)+y)$ be a function defined on $\mathbb{F}^* \times \mathbb{F}^*$, where $g,h\colon \mathbb{F}^* \to \mathbb{F}^*$ are arbitrary functions. Define $m = \mu(g\cdot h)$. For any subsets $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}^*$ with $|\mathscr{A}|,|\mathscr{B}|,|\mathscr{C}| \le p^{5/8}$, we have*

$$\max\{|f(\mathscr{A},\mathscr{B})|,|\mathscr{B}\cdot\mathscr{C}|\} \gg \min\left\{\frac{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}}{m^{\frac{4}{5}}}, \frac{|\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}}{m^{\frac{2}{3}}}\right\}.$$

The following are consequences of Theorem 8.1.3.

Corollary 8.1.4. *Let $f(x,y) = g(x)(h(x)+y)$ be a function defined on $\mathbb{F}^* \times \mathbb{F}^*$, where $g,h\colon \mathbb{F}^* \to \mathbb{F}^*$ are arbitrary functions with $\mu(g\cdot h) = O(1)$. For any subset $\mathscr{A} \subset \mathbb{F}^*$ with $|\mathscr{A}| \le p^{5/8}$, we have*

$$\max\{|f(\mathscr{A},\mathscr{A})|,|\mathscr{A}\cdot\mathscr{A}|\} \gg |\mathscr{A}|^{\frac{6}{5}}.$$

Corollary 8.1.5. *For $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}|,|\mathscr{B}|,|\mathscr{C}| \le p^{5/8}$.*

1. *Suppose that $g(x) = 1$ and $h(x) = 1/x$, then we have*

$$\max\{|\mathscr{A}^{-1}+\mathscr{B}|,|\mathscr{B}\cdot\mathscr{C}|\} \gg \min\left\{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}, |\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}, |\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}, |\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}\right\}.$$

2. *Suppose that $g(x) = x$ and $h(x) = 1$, then we have*

$$\max\{|\mathscr{A}(\mathscr{B}+1)|,|\mathscr{B}\cdot\mathscr{C}|\} \gg \min\left\{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}, |\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}, |\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}, |\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}\right\}.$$

This corollary is also an improvement of a recent result due to Zhelezov [96]. It follows from Corollary 8.1.5(2) that if $\mathscr{B} = \mathscr{A}$ and $\mathscr{C} = \mathscr{A}+1$ then we have $|\mathscr{A}(\mathscr{A}+1)| \gg |\mathscr{A}|^{6/5}$, which recovers the result of Stevens and de Zeeuw [76].

Our next result is the additive version of Theorem 8.1.3, which improves Theorem 8.1.2.

Theorem 8.1.6. *Let $f(x,y) = g(x)(h(x)+y)$ be a function defined on $\mathbb{F}^* \times \mathbb{F}^*$, where $g,h\colon \mathbb{F}^* \to \mathbb{F}^*$ are arbitrary functions. Define $m = \mu(g)$. For any subsets $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}^*$ with $|\mathscr{A}|,|\mathscr{B}|,|\mathscr{C}| \le p^{5/8}$, we have*

$$\max\{|f(\mathscr{A},\mathscr{B})|,|\mathscr{B}+\mathscr{C}|\} \gg \min\left\{\frac{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}}{m^{\frac{4}{5}}}, \frac{|\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}}{m^{\frac{2}{3}}}\right\}.$$

Corollary 8.1.7. *Let $f(x,y) = g(x)(h(x)+y)$ be a function defined on $\mathbb{F}^* \times \mathbb{F}^*$, where $g\colon \mathbb{F}^* \to \mathbb{F}^*$ are arbitrary functions with $\mu(g) = O(1)$. For any subset $\mathscr{A} \subset \mathbb{F}^*$ with $|\mathscr{A}| \leq p^{5/8}$, we have*

$$\max\left\{|f(\mathscr{A},\mathscr{A})|, |\mathscr{A}+\mathscr{A}|\right\} \gg |\mathscr{A}|^{\frac{6}{5}}.$$

Let $g(x) = x$ and $h(x) = 1$, we have the following corollary.

Corollary 8.1.8. *For $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}|, |\mathscr{B}|, |\mathscr{C}| \leq p^{5/8}$, we have*

$$\max\{|\mathscr{A}(\mathscr{B}+1)|, |\mathscr{B}+\mathscr{C}|\} \gg \min\left\{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}, |\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}, |\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}, |\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}\right\}.$$

In the case $g(x) = x$ and $h(x) = 0$, we have the following result.

Corollary 8.1.9. *For $\mathscr{A},\mathscr{B},\mathscr{C} \subset \mathbb{F}$ with $|\mathscr{A}|, |\mathscr{B}|, |\mathscr{C}| \ll p^{5/8}$, we have*

$$\max\{|\mathscr{A}\cdot\mathscr{B}|, |\mathscr{B}+\mathscr{C}|\} \gg \min\left\{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}, |\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}, |\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}, |\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}\right\}.$$

In the case $\mathscr{A} = \mathscr{B} = \mathscr{C}$, we recover the following result due to Roche-Newton, Rudnev, and Shkredov [64], which says that $\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \gg |\mathscr{A}|^{6/5}$.

It has been shown in [76] that if $f(x,y) = x(x+y)$, then $|f(\mathscr{A},\mathscr{A})| \gg |\mathscr{A}|^{5/4}$ under the condtion $|\mathscr{A}| \leq p^{2/3}$. In the following theorem, we show that if either $|\mathscr{A}+\mathscr{A}|$ or $|\mathscr{A}\cdot\mathscr{A}|$ is sufficiently small, the exponent $5/4$ can be improved from the polynomials to a larger family of function on $\mathbb{F}^* \times \mathbb{F}^*$

Theorem 8.1.10. *Let $f(x,y) = g(x)(h(x)+y)$ be a function defined on $\mathbb{F}^* \times \mathbb{F}^*$, where $g,h\colon \mathbb{F}^* \to \mathbb{F}^*$ are arbitrary functions with $\mu(f), \mu(g) = O(1)$. Consider the subset $\mathscr{A} \subset \mathbb{F}^*$ with $|\mathscr{A}| \leq p^{5/8}$, satisfying*

$$\min\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \leq |\mathscr{A}|^{\frac{9}{8}-\varepsilon},$$

for some $\varepsilon > 0$. Then, we have

$$|f(\mathscr{A},\mathscr{A})| \gg |\mathscr{A}|^{\frac{5}{4}+\frac{2\varepsilon}{3}}.$$

8.2 Proofs of Theorems 8.1.3, 8.1.6, and 8.1.10

Let $\mathscr{R}$ be a set of points in $\mathbb{F}^3$ and $\mathscr{S}$ be a set of planes in $\mathbb{F}^3$. We write $\mathscr{I}(\mathscr{R},\mathscr{S}) = |\{(r,s) \in \mathscr{R}\times\mathscr{S} : r \in s\}|$ for the number of *incidences* between $\mathscr{R}$ and $\mathscr{S}$. To prove Theorems 8.1.3 and 8.1.6, we make use of the following point-plane incidence bound due to Rudnev [66]. A short proof can be found in [20].

Theorem 8.2.1 (**Rudnev**, [66]). *Let $\mathscr{R}$ be a set of points in $\mathbb{F}^3$ and let $\mathscr{S}$ be a set of planes in $\mathbb{F}^3$, with $|\mathscr{R}| \ll |\mathscr{S}|$ and $|\mathscr{R}| \ll p^2$. Assume that there is no line containing k points of $\mathscr{R}$. Then*

$$\mathscr{I}(\mathscr{R},\mathscr{S}) \ll |\mathscr{R}|^{1/2}|\mathscr{S}| + k|\mathscr{S}|.$$

Proof of Theorem 8.1.3: Define $f(\mathscr{A},\mathscr{B}) = \{f(a,b)\colon a \in \mathscr{A}, b \in \mathscr{B}\}$, $g(\mathscr{A}) = \{g(a)\colon a \in \mathscr{A}\}$, $h(\mathscr{A}) = \{h(a)\colon a \in \mathscr{A}\}$. For $\lambda \in \mathscr{B}\cdot\mathscr{C}$, let

$$E_\lambda = \left|\left\{\left(f(a,b), c\cdot g(a)^{-1}, c\cdot h(a)\right)\colon (a,b,c) \in \mathscr{A}\times\mathscr{B}\times\mathscr{C},\ f(a,b)\cdot c\cdot g(a)^{-1} - c\cdot h(a) = \lambda\right\}\right|,$$

where by $g(a)^{-1}$ we mean the multiplicative inverse of $g(a)$ in $\mathbb{F}^*$. For a given triple $(x,y,z) \in (\mathbb{F}^*)^3$, we count the number of solutions $(a,b,c) \in \mathscr{A}\times\mathscr{B}\times\mathscr{C}$ to the following system

$$g(a)(h(a)+b) = x,\ c\cdot g(a)^{-1} = y,\ c\cdot h(a) = z.$$

This implies that

$$g(a)h(a) = zy^{-1}.$$

Since $\mu(g\cdot h) = m$, there are at most m different values of a satisfying the equation $g(a)h(a) = zy^{-1}$, and b,c are uniquely determined in term of a by the first and second equations of the system. This implies that

$$|\mathscr{A}||\mathscr{B}||\mathscr{C}|/m \le \sum_{\lambda\in\mathscr{B}\cdot\mathscr{C}} E_\lambda.$$

By the Cauchy-Schwarz inequality, we get

$$(|\mathscr{A}||\mathscr{B}||\mathscr{C}|/m)^2 \le \left(\sum_{\lambda\in\mathscr{B}\cdot\mathscr{C}} E_\lambda\right)^2 \le E\cdot|\mathscr{B}\cdot\mathscr{C}|, \tag{8.2.1}$$

where $E = \sum_{\lambda\in\mathscr{B}\cdot\mathscr{C}} E_\lambda^2$.

Define the point set $\mathscr{R}$ as

$$\mathscr{R} := \left\{\left(c\cdot g(a)^{-1}, c\cdot h(a), g(a')(h(a')+b')\right)\colon a,a' \in \mathscr{A}, b' \in \mathscr{B}, c \in \mathscr{C}\right\}$$

and the set of planes $\mathscr{S}$ as

$$\mathscr{S} := \left\{g(a)(h(a)+b)X - Y - c'g(a')^{-1}Z = -c'\cdot h(a')\colon a,a' \in \mathscr{A}, b \in \mathscr{B}, c' \in \mathscr{C}\right\}.$$

We have $E \le I(\mathscr{R},\mathscr{S})$, and $|\mathscr{R}| = |\mathscr{S}| \le |f(\mathscr{A},\mathscr{B})||\mathscr{A}||\mathscr{C}|$. To apply Theorem 8.2.1, we need to find an upper bound on k which is the maximum number of collinear points

in $\mathscr{R}$. The projection of $\mathscr{R}$ into the first two coordinates is the set $\mathscr{T} = \{(c \cdot g(a)^{-1}, c \cdot h(a)) : a \in \mathscr{A}, c \in \mathscr{C}\}$. The set $\mathscr{T}$ can be covered by the lines of the form $y = g(a)h(a)x$ with $a \in \mathscr{A}$. This implies that $\mathscr{T}$ can be covered by at most $|\mathscr{A}|$ lines passing through the origin, with each line containing $|\mathscr{C}|$ points of $\mathscr{T}$. Therefore, a line in $\mathbb{F}^3$ contains at most $\max\{|\mathscr{A}|, |\mathscr{C}|\}$ points of $\mathscr{R}$, unless it is vertical, in which case it contains at most $|f(\mathscr{A}, \mathscr{B})|$ points. In other words, we get

$$k \leq \max\{|\mathscr{A}|, |\mathscr{C}|, |f(\mathscr{A}, \mathscr{B})|\}.$$

If $|\mathscr{R}| \gg p^2$, then we get $|f(\mathscr{A}, \mathscr{B})||\mathscr{A}||\mathscr{C}| \gg p^2$. Since $|\mathscr{A}|, |\mathscr{C}| \leq p^{5/8}$, we have $|f(\mathscr{A}, \mathscr{B})| \gg p^{3/4} \gg |\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}$, and we are done in this case. Thus, we can assume that $|\mathscr{R}| \ll p^2$. Applying Theorem 8.2.1, we obtain

$$I(\mathscr{R}, \mathscr{S}) \leq |f(\mathscr{A}, \mathscr{B})|^{3/2}|\mathscr{A}|^{3/2}|\mathscr{C}|^{3/2} + k|f(\mathscr{A}, \mathscr{B})|\mathscr{A}||\mathscr{C}|. \tag{8.2.2}$$

Putting (8.2.1) and (8.2.2) together gives us

$$\max\left\{|f(\mathscr{A}, \mathscr{B})|, |\mathscr{B} \cdot \mathscr{C}|\right\} \gg \min\left\{\frac{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}}{m^{\frac{4}{5}}}, \frac{|\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}}{m}, \frac{|\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}}{m^{\frac{2}{3}}}\right\}.$$

This completes the proof of the theorem. □

Proof of Theorem 8.1.6: The proof goes in the same direction as Theorem 8.1.3, but for the sake of completeness, we include the detailed proof. For $\lambda \in \mathscr{B} + \mathscr{C}$, let

$$E_\lambda = \left|\left\{\left(f(a,b), g(a)^{-1}, c - h(a)\right) : (a,b,c) \in \mathscr{A} \times \mathscr{B} \times \mathscr{C},\ f(a,b) \cdot g(a)^{-1} + (c - h(a)) = \lambda\right\}\right|.$$

For a given triple $(x, y, z) \in (\mathbb{F}^*)^3$, we count the number of solutions $(a, b, c) \in \mathscr{A} \times \mathscr{B} \times \mathscr{C}$ to the following system

$$g(a)(h(a) + b) = x,\ g(a)^{-1} = y,\ c - h(a) = z.$$

Since $\mu(g) = m$, there are at most m different values of a satisfying the equation $g(a) = y^{-1}$, and b, c are uniquely determined in term of a by the first and third equations of the system. This implies that

$$|\mathscr{A}||\mathscr{B}||\mathscr{C}|/m \leq \sum_{\lambda \in \mathscr{B}+\mathscr{C}} E_\lambda.$$

By the Cauchy-Schwarz inequality, we have

$$(|\mathscr{A}||\mathscr{B}||\mathscr{C}|/m)^2 \leq \left(\sum_{\lambda\in\mathscr{B}+\mathscr{C}} E_\lambda\right)^2 \leq E\cdot|\mathscr{B}+\mathscr{C}|, \tag{8.2.3}$$

where $E=\sum_{\lambda\in\mathscr{B}+\mathscr{C}} E_\lambda^2$. Define the point set $\mathscr{R}$ as

$$\mathscr{R}:=\left\{\left(g(a)^{-1},c-h(a),g(a')(h(a')+b')\right): a,a'\in\mathscr{A},b'\in\mathscr{B},c\in\mathscr{C}\right\},$$

and the collection of planes $\mathscr{S}$ as

$$\mathscr{S}=\left\{g(a)(h(a)+b)X+Y-g(a')^{-1}Z=c'-h(a')\colon a,a'\in\mathscr{A},b\in\mathscr{B},c'\in\mathscr{C}\right\}.$$

It is clear that $|\mathscr{R}|=|\mathscr{S}|\leq|f(\mathscr{A},\mathscr{B})||\mathscr{A}||\mathscr{C}|$, and $E\leq I(\mathscr{R},\mathscr{S})$. To apply Theorem 8.2.1, we need to find an upper bound on k which is the maximum number of collinear points in $\mathscr{R}$. The projection of $\mathscr{R}$ into the first two coordinates is the set $\mathscr{T}=\{\left(g(a)^{-1},c-h(a)\right): a\in\mathscr{A},c\in\mathscr{C}\}$. The set $\mathscr{T}$ can be covered by at most $|\mathscr{A}|$ lines of the form $x=g(a)^{-1}$ with $a\in\mathscr{A}$, where each line contains $|\mathscr{C}|$ points of $\mathscr{T}$. Therefore, a line in $\mathbb{F}^3$ contains at most $\max\{|\mathscr{A}|,|\mathscr{C}|\}$ points of $\mathscr{R}$, unless it is vertical, in which case it contains at most $|f(\mathscr{A},\mathscr{B})|$ points. So we get

$$k\leq\max\{|\mathscr{A}|,|\mathscr{C}|,|f(\mathscr{A},\mathscr{B})|\}.$$

If $|\mathscr{R}|\gg p^2$, this implies that $|f(\mathscr{A},\mathscr{B})||\mathscr{A}||\mathscr{C}|\gg p^2$. Since $|\mathscr{A}|,|\mathscr{C}|\leq p^{5/8}$, we have $|f(\mathscr{A},\mathscr{B})|\gg p^{3/4}\gg|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}$, and we are done. Thus, we can assume that $|\mathscr{R}|\ll p^2$. Applying Theorem 8.2.1, we obtain

$$I(\mathscr{R},\mathscr{S})\leq|f(\mathscr{A},\mathscr{B})|^{3/2}|\mathscr{A}|^{3/2}|\mathscr{C}|^{3/2}+k|f(\mathscr{A},\mathscr{B})|\mathscr{A}||\mathscr{C}|. \tag{8.2.4}$$

Putting (8.2.3) and (8.2.4) together gives us

$$\max\left\{|f(\mathscr{A},\mathscr{B})|,|\mathscr{B}+\mathscr{C}|\right\}\gg\min\left\{\frac{|\mathscr{A}|^{\frac{1}{5}}|\mathscr{B}|^{\frac{4}{5}}|\mathscr{C}|^{\frac{1}{5}}}{m^{\frac{4}{5}}},\frac{|\mathscr{B}||\mathscr{C}|^{\frac{1}{2}}}{m},\frac{|\mathscr{B}||\mathscr{A}|^{\frac{1}{2}}}{m},\frac{|\mathscr{B}|^{2/3}|\mathscr{C}|^{1/3}|\mathscr{A}|^{1/3}}{m^{\frac{2}{3}}}\right\}.$$

This completes the proof. □

Proof of Theorem 8.1.10: One can assume that $|f(\mathscr{A},\mathscr{A})|\leq|\mathscr{A}|^2$, since otherwise we are done. Now by the proofs of Theorems 8.1.3 and 8.1.6 for $\mathscr{A}\subset\mathbb{F}^*$ with $|\mathscr{A}|\leq p^{5/8}$, we have

$$|f(\mathscr{A},\mathscr{A})|^{3/2}|\mathscr{A}\cdot\mathscr{A}|\gg|\mathscr{A}|^3,\ |f(\mathscr{A},\mathscr{A})|^{3/2}|\mathscr{A}+\mathscr{A}|\gg|\mathscr{A}|^3.$$

Since $\min\{|\mathscr{A}+\mathscr{A}|,|\mathscr{A}\cdot\mathscr{A}|\} \leq |\mathscr{A}|^{\frac{9}{8}-\varepsilon}$, we get $|f(\mathscr{A},\mathscr{A})|^{3/2} \gg |\mathscr{A}|^{3-\frac{9}{8}+\varepsilon}$, which concludes the proof of the theorem. □

9 Sum-product estimates over finite quasifields

9.1 Introduction

Let R be a ring and $\mathscr{A} \subset R$. The *sumset* of $\mathscr{A}$ is the set $\mathscr{A}+\mathscr{A} = \{a+b : a,b \in \mathscr{A}\}$, and the *product set* of $\mathscr{A}$ is the set $\mathscr{A}\cdot\mathscr{A} = \{a\cdot b : a,b \in \mathscr{A}\}$. A well-studied problem in arithmetic combinatorics is to prove non-trivial lower bounds on the quantity

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\}$$

under suitable hypothesis on R and $\mathscr{A}$. One of the first results of this type is due to Erdős and Szemerédi [26]. They proved that if $R = \mathbb{Z}$ and $\mathscr{A}$ is finite, then there are positive constants c and ε, both independent of $\mathscr{A}$, such that

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq c|\mathscr{A}|^{1+\varepsilon}.$$

This improves the trivial lower bound of $\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq |\mathscr{A}|$. Erdős and Szemerédi conjectured that the correct exponent is $2-o(1)$ where $o(1) \to 0$ as $|\mathscr{A}| \to \infty$. Despite a significant amount of research on this problem, this conjecture is still open. For some time the best known exponent was $4/3 - o(1)$ due to Solymosi [72] (see also [47] for similar results) who proved that for any finite set $\mathscr{A} \subset \mathbb{R}$,

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq \frac{|\mathscr{A}|^{4/3}}{2(\log|\mathscr{A}|)^{1/3}}.$$

Very recently, Konyagin and Shkredov [48] announced an improvement of the exponent to $4/3 + c - o(1)$ for any $c < \frac{1}{20598}$.

Another case that has received attention is when R is a finite field. Let p be a prime and let $\mathscr{A} \subset \mathbb{Z}_p$. As mentioned in the previous chapter, Bourgain, Katz, and Tao [9]

proved that if $p^\delta < |\mathscr{A}| < p^{1-\delta}$ where $0 < \delta < 1/2$, then

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq c|\mathscr{A}|^{1+\varepsilon} \tag{9.1.1}$$

for some positive constants c and ε depending only on δ. The current best bound for the case $|\mathscr{A}| \leq p^{5/8}$ was given by Roche-Newton, Rudnev, and Shkredov in [64]. For the case of large sets, Hart, Iosevich, and Solymosi [36] obtained bounds that give an explicit dependence of ε on δ. Let q be a power of an odd prime, $\mathbb{F}_q$ be the finite field with q elements, and $\mathscr{A} \subset \mathbb{F}_q$. In [36], it is shown that if $|\mathscr{A}+\mathscr{A}| = m$ and $|\mathscr{A}\cdot\mathscr{A}| = n$, then

$$|\mathscr{A}|^3 \leq \frac{cm^2n|\mathscr{A}|}{q} + cq^{1/2}mn \tag{9.1.2}$$

where c is some positive constant. Inequality (9.1.2) implies a non-trival sum-product estimate when $q^{1/2} \ll |\mathscr{A}| \ll q$. We write $f \ll g$ if $f = o(g)$. Using a graph theoretic approach, Vinh [85] and Vu [95] improved (9.1.2) and as a result, obtained a better sum-product estimate.

Theorem 9.1.1 ([85])**.** *Let q be a power of an odd prime. If $\mathscr{A} \subset \mathbb{F}_q$, $|\mathscr{A}+\mathscr{A}| = m$, and $|\mathscr{A}\cdot\mathscr{A}| = n$, then*

$$|\mathscr{A}|^2 \leq \frac{mn|\mathscr{A}|}{q} + q^{1/2}\sqrt{mn}.$$

Corollary 9.1.2 ([85])**.** *If q is a power of an odd prime and $\mathscr{A} \subset \mathbb{F}_q$, then there is a positive constant c such that the following hold. If $q^{1/2} \ll |\mathscr{A}| < q^{2/3}$, then*

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq \frac{c|\mathscr{A}|^2}{q^{1/2}}.$$

If $q^{2/3} \leq |\mathscr{A}| \ll q$, then

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq c(q|\mathscr{A}|)^{1/2}.$$

In the case that q is a prime, Corollary 9.1.2 was proved by Garaev [27] using exponential sums and Rudnev gave an estimate for small sets [65]. Cilleruelo [14] also proved related results using dense Sidon sets in finite groups involving $\mathbb{F}_q$ and $\mathbb{F}_q^*$. In particular, versions of Theorem 9.1.3 and (9.1.3) (see below) are proved in [14], as well as several other results concerning equations in $\mathbb{F}_q$ and sum-product estimates.

Theorem 9.1.1 was proved using the following Szemerédi-Trotter type theorem in $\mathbb{F}_q$.

Theorem 9.1.3 ([85])**.** *Let q be a power of an odd prime. If P is a set of points and L is a*

set of lines in $\mathbb{F}_q^2$*, then*

$$|\{(p,l) \in P \times L : p \in l\}| \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|}.$$

We remark that a Szemerédi-Trotter type theorem in $\mathbb{Z}_p$ was obtained in [9] using the sum-product estimate (9.1.1).

In this chapter, we generalize Theorem 9.1.1, Corollary 9.1.2, and Theorem 9.1.3 to finite quasifields. We recall the definition of a quasifield now: A set L with a binary operation $\cdot$ is called a *loop* if

1. the equation $a \cdot x = b$ has a unique solution in x for every $a, b \in L$,
2. the equation $y \cdot a = b$ has a unique solution in y for every $a, b \in L$, and
3. there is an element $e \in L$ such that $e \cdot x = x \cdot e = x$ for all $x \in L$.

A *(left) quasifield* Q is a set with two binary operations $+$ and $\cdot$ such that $(Q,+)$ is a group with additive identity 0, $(Q^*,\cdot)$ is a loop where $Q^* = Q\backslash\{0\}$, and the following three conditions hold:

1. $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in Q$,
2. $0 \cdot x = 0$ for all $x \in Q$, and
3. the equation $a \cdot x = b \cdot x + c$ has exactly one solution for every $a, b, c \in Q$ with $a \neq b$.

Any finite field is a quasifield. There are many examples of quasifields which are not fields; see for example, Chapter 5 of [21] or Chapter 9 of [42]. Quasifields appear extensively in the theory of projective planes. We note that in particular, in a quasifield multiplication need not be commutative nor associative. Throughout the chapter we must be careful about which side multiplication takes place on, and be wary that multiplicative inverses need not exist on both sides. Nonassociativity of multiplication is a bigger problem. Previous research on sum-product estimates requires associativity of multiplication for tools such as Plünnecke's inequality (see for example, [79] for the most general known sum-product theorem, the proof of which uses associativity of multiplication throughout).

Theorem 9.1.4. *Let Q be a finite quasifield with q elements. If $\mathscr{A} \subset Q\setminus\{0\}$, $|\mathscr{A}+\mathscr{A}| = m$, and $|\mathscr{A}\cdot\mathscr{A}| = n$, then*

$$|\mathscr{A}|^2 \leq \frac{mn|\mathscr{A}|}{q} + q^{1/2}\sqrt{mn}.$$

Theorem 9.1.4 gives the following sum-product estimate.

Corollary 9.1.5. *Let Q be a finite quasifield with q elements and $\mathscr{A} \subset Q\setminus\{0\}$. There is a positive constant c such that the following hold.*

If $q^{1/2} \ll |\mathscr{A}| < q^{2/3}$, then

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq c\frac{|\mathscr{A}|^2}{q^{1/2}}.$$

If $q^{2/3} \leq |\mathscr{A}| \ll q$, then

$$\max\{|\mathscr{A}+\mathscr{A}|, |\mathscr{A}\cdot\mathscr{A}|\} \geq c(q|\mathscr{A}|)^{1/2}.$$

From Corollary 9.1.5 we conclude that any algebraic object that is rich enough to coordinatize a projective plane must satisfy a non-trivial sum-product estimate. Following [85], we prove a Szemerédi-Trotter type theorem and then use it to deduce Theorem 9.1.4. We note that the connection between arithmetic combinatorics and incidence geometry was studied in a general form in [28]. We also note that many authors have studied more general incidence theorems and their relationship to arithmetic combinatorics (cf [35, 40, 17, 18]).

Theorem 9.1.6. *Let Q be a finite quasifield with q elements. If P is a set of points and L is a set of lines in Q^2, then*

$$|\{(p,l) \in P\times L : p \in l\}| \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|}.$$

Another consequence of Theorem 9.1.6 is the following corollary.

Corollary 9.1.7. *If Q is a finite quasifield with q elements and $\mathscr{A} \subset Q$, then there is a positive constant c such that*

$$|\mathscr{A}\cdot(\mathscr{A}+\mathscr{A})| \geq c\min\left\{q, \frac{|\mathscr{A}|^3}{q}\right\}.$$

Further, if $|\mathscr{A}| \gg q^{2/3}$, then one may take $c = 1+o(1)$.

The next result generalizes Theorem 1.1 from [92].

Theorem 9.1.8. *Let Q be a finite quasifield with q elements. If $\mathscr{A},\mathscr{B},\mathscr{C} \subset Q$, then*

$$|\mathscr{A}+\mathscr{B}\cdot\mathscr{C}| \geq q - \frac{q^3}{|\mathscr{A}||\mathscr{B}||\mathscr{C}|+q^2}$$

We note that Corollary 9.1.7 applies to elements of the form $a\cdot b+a\cdot c$ where $a,b,c\in\mathscr{A}$ and Theorem 9.1.8 applies to elements of the form $a+b\cdot c$ where $a\in\mathscr{A}$, $b\in\mathscr{B}$, and $c\in\mathscr{C}$. Theorem 9.1.8 does not use our Szemerédi-Trotter Theorem, and its proof allows for the more general result of taking three distinct sets, whereas Corollary 9.1.7 is not as flexible, but gives a better estimate when $|\mathscr{A}|$ is between $q^{1/3}$ and $q^{2/3}$. The spirit of these two results is similar, though it is not clear in the setting of a quasifield that the sets $\mathscr{A}\cdot(\mathscr{A}+\mathscr{A})$ and $\mathscr{A}+\mathscr{A}\cdot\mathscr{A}$ should necessarily behave the same way (it is also not clear that they shouldn't).

Our methods in proving the above results can be used to generalize theorems concerning the solvability of equations over finite fields. Let p be a prime and let $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}\subset\mathbb{Z}_p$. Sárközy [67] proved that if $N(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D})$ is the number of solutions to $a+b=cd$ with $(a,b,c,d)\in\mathscr{A}\times\mathscr{B}\times\mathscr{C}\times\mathscr{D}$, then

$$\left|N(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}) - \frac{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{p}\right| \leq p^{1/2}\sqrt{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}. \tag{9.1.3}$$

In particular, if $|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|>p^3$, then there is an $(a,b,c,d)\in\mathscr{A}\times\mathscr{B}\times\mathscr{C}\times\mathscr{D}$ such that $a+b=cd$. This is best possible up to a constant factor (see [67]). It was generalized to finite fields of odd prime power order by Gyarmati and Sárközy [30], and then by the fourth author [84] to systems of equations over $\mathbb{F}_q$. Here we generalize the result of Gyarmati and Sárközy to finite quasifields.

Theorem 9.1.9. *Let Q be a finite quasifield with q elements and let $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}\subset Q$. If $\gamma\in Q$ and $N_\gamma(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D})$ is the number of solutions to $a+b+\gamma=c\cdot d$ with $a\in\mathscr{A}$, $b\in\mathscr{B}$, $c\in\mathscr{C}$, and $d\in\mathscr{D}$, then*

$$\left|N_\gamma(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}) - \frac{(q+1)|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{q^2+q+1}\right| \leq q^{1/2}\sqrt{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}.$$

Theorem 9.1.9 implies the following Corollary which generalizes Corollary 3.5 in [87].

Corollary 9.1.10. *If Q is a finite quasifield with q elements and $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}\subset Q$ with $|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|>q^3$, then*

$$Q=\mathscr{A}+\mathscr{B}+\mathscr{C}\cdot\mathscr{D}.$$

We also prove a higher dimensional version of Theorem 9.1.9.

Theorem 9.1.11. *Let $d \geq 1$ be an integer. If Q is a finite quasifield with q elements and $\mathscr{A} \subset Q$ with $|\mathscr{A}| \geq 2q^{\frac{d+2}{2d+2}}$, then*

$$Q = \mathscr{A} + \mathscr{A} + \underbrace{\mathscr{A}\cdot\mathscr{A} + \cdots + \mathscr{A}\cdot\mathscr{A}}_{d \text{ terms}}.$$

Another problem considered by Sárközy was the solvability of the equation $ab+1 = cd$ over $\mathbb{Z}_p$. Sárközy [68] proved a result in $\mathbb{Z}_p$ which was later generalized to the finite field setting in [30].

Theorem 9.1.12 (Gyarmati, Sárközy)**.** *Let q be a power of a prime and $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D} \subset \mathbb{F}_q$. If $N(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D})$ is the number of solutions to $ab+1 = cd$ with $a \in \mathscr{A}$, $b \in \mathscr{B}$, $c \in \mathscr{C}$, and $d \in \mathscr{D}$, then*

$$\left| N(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}) - \frac{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{q} \right| \leq 8q^{1/2}(|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|)^{1/2} + 4q^2.$$

Our generalization to quasifields is as follows.

Theorem 9.1.13. *Let Q be a finite quasifield with q elements and kernel K. Let $\gamma \in Q\backslash\{0\}$, and $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D} \subset Q$. If $N_\gamma(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D})$ is the number of solutions to $a\cdot b + c\cdot d = \gamma$, then*

$$\left| N_\gamma(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}) - \frac{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{q} \right| \leq q\left(\frac{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{|K|-1} \right)^{1/2}.$$

Corollary 9.1.14. *Let Q be a quasifield with q elements whose kernel is K. If $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D} \subset Q$ and $|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}| > q^4(|K|-1)^{-1}$, then*

$$Q\backslash\{0\} \subset \mathscr{A}\cdot\mathscr{B} + \mathscr{C}\cdot\mathscr{D}.$$

By appropriately modifying the argument used to prove Theorem 9.1.13, we can prove a higher dimensional version.

Theorem 9.1.15. *Let Q be a finite quasifield with q elements whose kernel is K. If $\mathscr{A} \subset Q$ and $|\mathscr{A}| > q^{\frac{1}{2}+\frac{1}{d}}(|K|-1)^{-1/2d}$, then*

$$Q\backslash\{0\} \subset \underbrace{\mathscr{A}\cdot\mathscr{A} + \cdots + \mathscr{A}\cdot\mathscr{A}}_{d \text{ terms}}.$$

If Q is a finite field, then $|K| = q$, and the bounds of Theorems 9.1.13 and 9.1.15 match the bounds obtained by Hart and Iosevich in [33].

Finally, we note that our theorems are proved using spectral techniques. In the proofs, if the size of the set is small, the error term from spectral estimates will dominate. Therefore, the results presented are only nontrivial if the size of the set is large enough. Sum-product estimates for small sets have been given (for example in [9, 47, 79]). We also note that it is not hard to show that one may find a set $\mathscr{A}$ in either a field, general ring, or quasifield, where both $|\mathscr{A}+\mathscr{A}|$ and $|\mathscr{A}\cdot\mathscr{A}|$ are of order $|\mathscr{A}|^2$.

The rest of the chapter is organized as follows. In Section 2 we collect some preliminary results. Section 3 contains the proof of Theorem 9.1.4, 9.1.6, and 9.1.9, as well as Corollary 9.1.5, 9.1.7, and 9.1.10. Section 4 contains the proof of Theorem 9.1.8 and 9.1.11. Section 5 contains the proof of Theorem 9.1.13 and 9.1.15.

9.2 Preliminaries

We begin this section by giving some preliminary results on quasifields. Let Q denote a finite quasifield. We use 1 to denote the identity in the loop $(Q^*,\cdot)$. It is a consequence of the definition that $(Q,+)$ must be an abelian group. One also has $x\cdot 0 = 0$ and $x\cdot(-y) = -(x\cdot y)$ for all $x,y\in Q$ (see [42], Lemma 7.1). For more on quasifields, see Chapter 9 of [42]. A *(right) quasifield* is required to satisfy the right distributive law instead of the left distributive law. The *kernel* K of a quasifield Q is the set of all elements $k\in Q$ that satisfy

1. $(x+y)\cdot k = x\cdot k + y\cdot k$ for all $x,y\in Q$, and
2. $(x\cdot y)\cdot k = x\cdot(y\cdot k)$ for all $x,y\in Q$.

Note that $(K,+)$ is an abelian subgroup of $(Q,+)$ and $(K^*,\cdot)$ is a group.

Lemma 9.2.1. *If $a\in Q$ and $\lambda\in K$, then $-(a\cdot\lambda) = (-a)\cdot\lambda$.*

Proof. First we show that $a\cdot(-1) = -a$. Indeed, $a\cdot(1+(-1)) = a\cdot 0 = 0$ and so $a+a\cdot(-1) = 0$. We conclude that $-a = a\cdot(-1)$. If $\lambda\in K$, then

$$\begin{aligned} -(a\cdot\lambda) &= a\cdot(-\lambda) = a\cdot(0-\lambda) = a\cdot((0-1)\cdot\lambda) \\ &= (a\cdot(0-1))\cdot\lambda = (0+a\cdot(-1))\cdot\lambda = (-a)\cdot\lambda. \end{aligned}$$

□

For the rest of this section, we assume that Q is a finite quasifield with $|Q| = q$. We can construct a projective plane $\Pi = (\mathscr{P},\mathscr{L},\mathscr{I})$ that is coordinatized by Q. Here $\mathscr{I}\subset\mathscr{P}\times\mathscr{L}$

is the set of *incidences* between points and lines. If $p \in \mathscr{P}$ and $l \in \mathscr{L}$, we write $p \mathscr{I} l$ to denote that $(p,l) \in \mathscr{I}$, ie that p is incident with l. We will follow the notation of [42] and refer the reader to Chapter 5 of [42] for more details. Let ∞ be a symbol not in Q. The points of Π are defined as

$$\mathscr{P} = \{(x,y) : x,y \in Q\} \cup \{(x) : x \in Q\} \cup \{(\infty)\}.$$

The lines of Π are defined as

$$\mathscr{L} = \{[m,k] : m,k \in Q\} \cup \{[m] : m \in Q\} \cup \{[\infty]\}.$$

The incidence relation $\mathscr{I}$ is defined according to the following rules:

1. $(x,y)\mathscr{I}[m,k]$ if and only if $m \cdot x + y = k$,
2. $(x,y)\mathscr{I}[k]$ if and only if $x = k$,
3. $(x)\mathscr{I}[m,k]$ if and only if $x = m$,
4. $(x)\mathscr{I}[\infty]$ for all $x \in Q$, $(\infty)\mathscr{I}[k]$ for all $k \in Q$, and $(\infty)\mathscr{I}[\infty]$.

Since $|Q| = q$, the plane Π has order q.

Next we associate a graph to the plane Π. Let $\mathscr{G}(\Pi)$ be the bipartite graph with parts $\mathscr{P}$ and $\mathscr{L}$ where $p \in \mathscr{P}$ is adjacent to $l \in \mathscr{L}$ if and only if $p \mathscr{I} l$ in Π. The first lemma is known (see [10], page 432).

Lemma 9.2.2. *The graph $\mathscr{G}(\Pi)$ has eigenvalues $q+1$ and $-(q+1)$, each with multiplicity one. All other eigenvalues of $\mathscr{G}(\Pi)$ are $\pm q^{1/2}$.*

The next lemma is a bipartite version of the well-known Expander Mixing Lemma.

Lemma 9.2.3 (Bipartite Expander Mixing Lemma)**.** *Let G be a d-regular bipartite graph on $2n$ vertices with parts X and Y. Let M be the adjacency matrix of G. Let $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{2n} = -d$ be the eigenvalues of M and define $\lambda = \max_{i \neq 1,2n} |\lambda_i|$. Let $S \subset X$ and $T \subset Y$, and let $e(S,T)$ denote the number of edges with one endpoint in S and the other in T. Then*

$$\left| e(S,T) - \frac{d|S||T|}{n} \right| \leq \lambda \sqrt{|S||T|}.$$

Proof. Assume that the columns of M have been been ordered so that the columns corresponding to the vertices of X come before the columns corresponding to the

vertices of Y. For a subset $\mathscr{B} \subset V(G)$, let $\chi_{\mathscr{B}}$ be the characteristic vector for $\mathscr{B}$. Let $\{x_1, \ldots, x_{2n}\}$ be an orthonormal set of eigenvectors for M. Note that since G is a d-regular bipartite graph, we have

$$x_1 = \frac{1}{\sqrt{2n}}\left(\chi_X + \chi_Y\right), \tag{9.2.1}$$

$$x_{2n} = \frac{1}{\sqrt{2n}}\left(\chi_X - \chi_Y\right). \tag{9.2.2}$$

Now $\chi_S^T M \chi_T = e(S,T)$. Expanding χ_S and χ_T as linear combinations of eigenvectors yields

$$e(S,T) = \left(\sum_{i=1}^{2n} \langle \chi_S, x_i\rangle x_i\right)^T M \left(\sum_{i=1}^{2n} \langle \chi_T, x_i\rangle x_i\right) = \sum_{i=1}^{2n} \langle \chi_S, x_i\rangle \langle \chi_T, x_i\rangle \lambda_i.$$

Now by (9.2.1) and (9.2.2), $\langle \chi_S, x_1\rangle = \langle \chi_S, x_{2n}\rangle = \frac{1}{\sqrt{2n}}|S|$ and $\langle \chi_T, x_1\rangle = -\langle \chi_T, x_{2n}\rangle = \frac{1}{\sqrt{2n}}|T|$. Since $\lambda_1 = -\lambda_{2n} = d$, we have

$$\begin{aligned}
\left|e(S,T) - \frac{2d|S||T|}{2n}\right| &= \left|\sum_{i=2}^{2n-1} \langle \chi_S, x_i\rangle \langle \chi_T, x_i\rangle \lambda_i\right| \\
&\leq \lambda \sum_{i=2}^{2n-1} \left|\langle \chi_S, x_i\rangle \langle \chi_T, x_i\rangle\right| \\
&\leq \lambda \left(\sum_{i=2}^{2n-1} \langle \chi_S, x_i\rangle^2\right)^{1/2} \left(\sum_{i=2}^{2n-1} \langle \chi_T, x_i\rangle^2\right)^{1/2} \quad \text{(by Cauchy-Schwarz).}
\end{aligned}$$

Finally by the Pythagorean Theorem,

$$\sum_{i=2}^{2n-1} \langle \chi_S, x_i\rangle^2 = |S| - \frac{2|S|^2}{2n} < |S|$$

and

$$\sum_{i=2}^{2n-1} \langle \chi_T, x_i\rangle^2 = |T| - \frac{2|T|^2}{2n} < |T|.$$

□

Combining Lemmas 9.2.2 and 9.2.3 gives the next lemma.

Lemma 9.2.4. *For any $S \subset \mathscr{P}$ and $T \subset \mathscr{L}$,*

$$\left|e(S,T) - \frac{(q+1)|S||T|}{q^2+q+1}\right| \leq q^{1/2}\sqrt{|S||T|}$$

where $e(S,T)$ is the number of edges in $\mathcal{G}(\Pi)$ with one endpoint in S and the other in T.

We now state precisely what we mean by a line in Q^2.

Definition 4. *Given $a,b \in Q$, a line in Q^2 is a set of the form*

$$\{(x,y) \in Q^2 : y = b\cdot x + a\} \text{ or } \{(a,y) : y \in Q\}.$$

When multiplication is commutative, $b\cdot x + a = x\cdot b + a$. In general, the binary operation $\cdot$ need not be commutative and so we write our lines with the slope on the left.

The next lemma is due to Elekes [22] (see also [78], page 315). In working in a (left) quasifield, which is not required to satisfy the right distributive law, some care must be taken with algebraic manipulations.

Lemma 9.2.5. *Let $\mathscr{A} \subset Q^*$. There is a set P of $|\mathscr{A}+\mathscr{A}||\mathscr{A}\cdot\mathscr{A}|$ points and a set L of $|\mathscr{A}|^2$ lines in Q^2 such that there are at least $|\mathscr{A}|^3$ incidences between P and L.*

Proof. Let $P = (\mathscr{A}+\mathscr{A}) \times (\mathscr{A}\cdot\mathscr{A})$ and

$$l(a,b) = \{(x,y) \in Q^2 : y = b\cdot x - b\cdot a\}.$$

Let $L = \{l(a,b) : a,b \in \mathscr{A}\}$. The statement that $|P| = |\mathscr{A}+\mathscr{A}||\mathscr{A}\cdot\mathscr{A}|$ is clear from the definition of P. Suppose $l(a,b)$ and $l(c,d)$ are elements of L and $l(a,b) = l(c,d)$. We claim that $(a,b) = (c,d)$. In a quasifield, one has $x\cdot 0 = 0$ for every x, and $x\cdot(-y) = -(x\cdot y)$ for every x and y ([42], Lemma 7.1). The line $l(a,b)$ contains the points $(0,-b\cdot a)$ and $(1,b-b\cdot a)$. Furthermore, these are the unique points in $l(a,b)$ with first coordinate 0 and 1, respectively. Similarly, the line $l(c,d)$ contains the points $(0,-d\cdot c)$ and $(1,d-d\cdot c)$. Since $l(a,b) = l(c,d)$, we must have that $-b\cdot a = -d\cdot c$ and $b - b\cdot a = d - d\cdot c$. Thus, $b = d$ and so $b\cdot a = b\cdot c$. We can rewrite this equation as $b\cdot a - b\cdot c = 0$. Since $-x\cdot y = x\cdot(-y)$ and Q satisfies the left distributive law, we have $b\cdot(a-c) = 0$. If $a = c$, then $(a,b) = (c,d)$ and we are done. Assume that $a \neq c$ so that $a - c \neq 0$. Then we must have $b = 0$ for if $b \neq 0$, then the product $b\cdot(a-c)$ would be contained in Q^* as multiplication is a binary operation on Q^*. Since $\mathscr{A} \subset Q^*$, we have $b \neq 0$. It must be the case that $a = c$. We conclude that each pair $(a,b) \in \mathscr{A}^2$ determines a unique line in L and so $|L| = |\mathscr{A}|^2$.

Consider a triple $(a,b,c) \in \mathscr{A}^3$. The point $(a+c, b\cdot c)$ belongs to P and is incident to $l(a,b) \in L$ since

$$b\cdot(a+c) - b\cdot a = b\cdot a + b\cdot c - b\cdot a = b\cdot c.$$

Each triple in $\mathscr{A}^3$ generates an incidence and so there are at least $|\mathscr{A}|^3$ incidences between P and L. □

9.3 Proofs of Theorems 9.1.4, 9.1.6, and 9.1.9

Throughout this section, Q is a finite quasifield with q elements, $\Pi = (\mathscr{P}, \mathscr{L}, \mathscr{I})$ is the the projective plane coordinatized by Q as in Section 2. The graph $\mathscr{G}(\Pi)$ is the bipartite graph defined before Lemma 9.2.2 in Section 2.

Proof of Theorem 9.1.6. Let $P \subset Q^2$ be a set of points and view P as a subset of $\mathscr{P}$. Let $r(a,b) = \{(x,y) \in Q^2 : y = b \cdot x + a\}$, $R \subset Q^2$, and let

$$L = \{r(a,b) : (a,b) \in R\}$$

be a collection of lines in Q^2. The point $p = (p_1, p_2)$ in P is incident to the line $r(a,b)$ in L if and only if $p_2 = b \cdot p_1 + a$. This however is equivalent to $(p_1, -p_2) \mathscr{I} [b, -a]$ in Π. If $S = \{(p_1, -p_2) : (p_1, p_2) \in P\}$ and $T = \{[b, -a] : (a,b) \in R\}$, then

$$|\{(p,l) \in P \times L : p \in l\}| = e(S,T)$$

where $e(S,T)$ is the number of edges in $\mathscr{G}(\Pi)$ with one endpoint in S and the other in T. By Lemma 9.2.4,

$$|\{(p,l) \in P \times L : p \in l\}| \leq \frac{|S||T|}{q} + q^{1/2}\sqrt{|S||T|}$$

which proves Theorem 9.1.6. □

Proof of Theorem 9.1.4 and Corollary 9.1.5. Let $\mathscr{A} \subset Q^*$. Let $S = (\mathscr{A} + \mathscr{A}) \times (\mathscr{A} \cdot \mathscr{A})$. We view S as a subset of $\mathscr{P}$. Let $s(a,b) = \{(x,y) \in Q^2 : y = b \cdot x - b \cdot a\}$ and

$$L = \{s(a,b) : a, b \in \mathscr{A}\}.$$

By Lemma 9.2.5, $|L| = |\mathscr{A}|^2$ and there are at least $|\mathscr{A}|^3$ incidences between S and L. Let $T = \{[-b, -b \cdot a] : a, b \in \mathscr{A}\}$ so T is a subset of $\mathscr{L}$. By Lemma 9.2.4,

$$e(S,T) \leq \frac{|S||T|}{q} + q^{1/2}\sqrt{|S||T|}.$$

We have $|L| = |T| = |\mathscr{A}|^2$. If $m = |\mathscr{A} + \mathscr{A}|$ and $n = |\mathscr{A} \cdot \mathscr{A}|$, then

$$e(S,T) \leq \frac{mn|\mathscr{A}|^2}{q} + q^{1/2}|\mathscr{A}|\sqrt{mn}.$$

Next we find a lower bound on $e(S,T)$. By construction, an incidence between S and L corresponds to an edge between S and T in $\mathscr{G}(\Pi)$. To see this, note that $(x,y) \in S$ is incident to $s(a,b) \in L$ if and only if $y = b \cdot x - b \cdot a$. This is equivalent to the equation $-b \cdot x + y = -b \cdot a$ which holds if and only if (x,y) is adjacent to $[-b, -b \cdot a]$ in $\mathscr{G}(\Pi)$. Thus,

$$|\mathscr{A}|^3 \leq e(S,T) \leq \frac{mn|\mathscr{A}|^2}{q} + q^{1/2}|\mathscr{A}|\sqrt{mn}. \tag{9.3.1}$$

To prove Corollary 9.1.5, observe that from (9.3.1), we have

$$|\mathscr{A} + \mathscr{A}||\mathscr{A} \cdot \mathscr{A}| \geq \min\left\{cq|\mathscr{A}|, \frac{c|\mathscr{A}|^4}{q}\right\}$$

where c is any real number with $c + c^{1/2} < 1$. If $x = \max\{|\mathscr{A} + \mathscr{A}|, |\mathscr{A} \cdot \mathscr{A}|\}$, then $x \geq \min\{(cq|\mathscr{A}|)^{1/2}, \frac{c^{1/2}|\mathscr{A}|^2}{q^{1/2}}\}$ and Corollary 9.1.5 follows from this inequality. □

Proof of Corollary 9.1.7. Let $\mathscr{A} \subset Q$, $P = \mathscr{A} \times (\mathscr{A} \cdot (\mathscr{A} + \mathscr{A}))$,

$$l(b,c) = \{(x,y) \in Q^2 : y = b \cdot (x + c)\},$$

and $L = \{l(b,c) : b, c \in \mathscr{A}\}$. Then $|P| = |\mathscr{A}||\mathscr{A} \cdot (\mathscr{A} + \mathscr{A})|$, $|L| = |\mathscr{A}|^2$, and L is a set of lines in Q^2. Let $z = |\mathscr{A} \cdot (\mathscr{A} + \mathscr{A})|$. Observe that each $l(b,c) \in L$ contains at least $|\mathscr{A}|$ points from P. By Theorem 9.1.6,

$$|\mathscr{A}|^3 \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|} = \frac{|\mathscr{A}|^3 z}{q} + q^{1/2}|\mathscr{A}|^{3/2}z^{1/2}.$$

This implies that $q|\mathscr{A}|^{3/2} \leq |\mathscr{A}|^{3/2}z + q^{3/2}\sqrt{z}$. Therefore, we obtain

$$\sqrt{z} \geq \frac{-q^{3/2} + \sqrt{q^3 + 4|\mathscr{A}|^3 q}}{2|\mathscr{A}|^{3/2}} = \frac{4|\mathscr{A}|^3 q}{2|\mathscr{A}|^{3/2}(q^{3/2} + \sqrt{q^3 + 4|\mathscr{A}|^3 q})},$$

which implies that

$$|\mathscr{A} \cdot (\mathscr{A} + \mathscr{A})| \geq c \min\left\{q, \frac{|\mathscr{A}|^3}{q}\right\}.$$

We note that if $|\mathscr{A}| \gg q^{2/3}$ then we can take $c = 1 + o(1)$. □

Proof of Theorem 9.1.9 and Corollary 9.1.10. Let $\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D} \subset Q$. Consider the sets $P = \{(d,-a) : d \in \mathscr{D}, a \in \mathscr{A}\}$ and $L = \{[c,b+\gamma] : c \in \mathscr{C}, b \in \mathscr{B}\}$. An edge between P and L in $\mathscr{G}(\Pi)$ corresponds to a solution to $c \cdot d + (-a) = b + \gamma$ with $c \in \mathscr{C}$, $d \in \mathscr{D}$, $a \in \mathscr{A}$, and $b \in \mathscr{B}$. Therefore, $e(P,L)$ is precisely the number of solutions to $a+b+\gamma = c \cdot d$ with $(a,b,c,d) \in \mathscr{A} \times \mathscr{B} \times \mathscr{C} \times \mathscr{D}$. Observe that $|P| = |\mathscr{D}||\mathscr{A}|$ and $|L| = |\mathscr{C}||\mathscr{B}|$. By Lemma 9.2.4,

$$\left| N_\gamma(\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{D}) - \frac{(q+1)|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{q^2+q+1} \right| \leq q^{1/2}\sqrt{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}.$$

To obtain Corollary 9.1.10, apply Theorem 9.1.9 with $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, and $-\mathscr{D}$. For any $-\gamma \in Q$, the number of $(a,b,c,-d) \in \mathscr{A} \times \mathscr{B} \times \mathscr{C} \times (-\mathscr{D})$ with $a+b-\gamma = c \cdot (-d)$ is at least

$$\frac{(q+1)|\mathscr{A}||\mathscr{B}||\mathscr{C}||-\mathscr{D}|}{q^2+q+1} - q^{1/2}\sqrt{|\mathscr{A}||\mathscr{B}||\mathscr{C}||-\mathscr{D}|}. \tag{9.3.2}$$

When $|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}| > q^3$, (9.3.2) is positive and so we have a solution to $a+b-\gamma = c\cdot(-d)$. Since this equation is equivalent to $a+b+c\cdot d = \gamma$ and γ was arbitrary, we get

$$Q = \mathscr{A} + \mathscr{B} + \mathscr{C} \cdot \mathscr{D}.$$

□

9.4 Proofs of Theorems 9.1.8 and 9.1.11

Let $\gamma \in Q$ and $d \geq 1$ be an integer. In order to prove Theorems 9.1.11 and 9.1.8, we will need to consider a graph that is different from $\mathscr{G}(\Pi)$. Define the product graph $\mathscr{SP}_Q(\gamma)$ to be the bipartite graph with parts X and Y where X and Y are disjoint copies of Q^{d+1}. The vertex $(x_1,\dots,x_{d+1})_X \in X$ is adjacent to the vertex $(y_1,\dots,y_{d+1})_Y \in Y$ if and only if

$$x_1 + y_1 + \gamma = x_2 \cdot y_2 + \cdots + x_{d+1} \cdot y_{d+1}. \tag{9.4.1}$$

Lemma 9.4.1. *For any $\gamma \in Q$ and integer $d \geq 1$, the graph $\mathscr{SP}_Q(\gamma)$ is q^d-regular.*

Proof. Let $(x_1,\dots,x_{d+1})_X$ be a vertex in X. Choose $y_2,\dots,y_{d+1} \in Q$ arbitrarily. Equation (9.4.1) has a unique solution for y_1 and so the degree of $(x_1,\dots,x_{d+1})_X$ is q^d. A similar argument applies to the vertices in Y. □

Lemma 9.4.2. *Let $\gamma \in Q$ and $d \geq 1$ be an integer. If $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of $\mathscr{SP}_Q(\gamma)$, then $\lambda \leq q^{d/2}(1+q^{-2})^{1/2}$ where $\lambda = \max_{i\neq 1,n}|\lambda_i|$.*

Proof. Let M be the adjacency matrix for $\mathscr{SP}_Q(\gamma)$ where the first q^{d+1} rows/columns are indexed by the elements of X. We can write

$$M = \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}$$

where N is the $q^{d+1} \times q^{d+1}$ matrix whose $(x_1,\dots,x_{d+1})_X \times (y_1,\dots,y_{d+1})_Y$ entry is 1 if

$$x_1 + y_1 + \gamma = x_2 \cdot y_2 + \cdots + x_{d+1} \cdot y_{d+1}$$

and is 0 otherwise.

Let $x = (x_1,\dots,x_{d+1})_X$ and $x' = (x'_1,\dots,x'_{d+1})_X$ be distinct vertices in X. The number of common neighbors of x and x' is the number of vertices $(y_1,\dots,y_{d+1})_Y$ such that

$$x_1 + y_1 + \gamma = x_2 \cdot y_2 + \cdots + x_{d+1} \cdot y_{d+1} \tag{9.4.2}$$

and

$$x'_1 + y_1 + \gamma = x'_2 \cdot y_2 + \cdots + x'_{d+1} \cdot y_{d+1}. \tag{9.4.3}$$

Subtracting (9.4.3) from (9.4.2) gives

$$x_1 - x'_1 = x_2 \cdot y_2 + \cdots + x_{d+1} \cdot y_{d+1} - x'_2 \cdot y_2 - \cdots - x'_{d+1} \cdot y_{d+1}. \tag{9.4.4}$$

If $x_i = x'_i$ for $2 \le i \le d+1$, then the right hand side of (9.4.4) is 0 so that $x_1 = x'_1$. This contradicts our assumption that x and x' are distinct vertices. Thus, there is an $i \in \{2,3,\dots,d+1\}$ for which $x_i \neq x'_i$. There are q^{d-2} choices for $y_2,\dots,y_{i-1},y_{i+1},\dots y_{d+1}$. Once these y_j's have been chosen, (9.4.4) uniquely determines y_i since $x_i - x'_i \neq 0$. Equation (9.4.2) then uniquely determines y_1. Therefore, x and x' have exactly q^{d-2} common neighbors when $x \neq x'$. A similar argument applies to the vertices in Y so that any two distinct vertices y and y' in Y have q^{d-2} common neighbors.

Let J be the $q^{d+1} \times q^{d+1}$ matrix of all 1's and I be the $2q^{d+1} \times 2q^{d+1}$ identity matrix. Let $\mathscr{B}_E$ be the graph whose vertex set is $X \cup Y$ and two vertices v and y in $\mathscr{B}_E$ are adjacent if and only if they are both in X or both in Y, and they have no common neighbor in the graph $\mathscr{SP}_Q(\gamma)$. The graph $\mathscr{B}_E$ is $(q-1)$-regular since given any $(d+1)$-tuple $(z_1,\dots,z_{d+1}) \in Q^{d+1}$, there are exactly $q-1$ $(d+1)$-tuples $(z'_1,\dots,z'_{d+1}) \in Q^{d+1}$ for which $z_1 \neq z'_1$ and $z_i = z'_i$ for $2 \le i \le d+1$. It follows that

$$M^2 = q^{d-2}\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix} + (q^d - q^{d-2})I - q^{d-2}E \tag{9.4.5}$$

where E is the adjacency matrix of $\mathscr{B}_E$.

By Lemma 9.4.1, the graph $\mathscr{SP}_Q(\gamma)$ is a q^d-regular bipartite graph so $\lambda_1 = q^d$, $\lambda_n = -q^d$, and the corresponding eigenvectors are $q^{d/2}(\chi_X + \chi_Y)$ and $q^{d/2}(\chi_X - \chi_Y)$, respectively. Here χ_Z denotes the characteristic vector for the set of vertices Z. Let λ_j be an eigenvalue of $\mathscr{SP}_Q(\gamma)$ with $j \neq 1$ and $j \neq n$. Assume that v_j is an eigenvector for λ_j. Since v_j is orthogonal to both $\chi_X + \chi_Y$ and $\chi_X - \chi_Y$, we have

$$\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix} v_j = 0.$$

By (9.4.5), $M^2 v_j = (q^d - q^{d-2}) v_j - q^{d-2} E v_j$ which can be rewritten as

$$E v_j = \left(q^2 - 1 - \frac{\lambda_j^2}{q^{d-2}} \right) v_j.$$

Thus, $q^2 - 1 - \frac{\lambda_j^2}{q^{d-2}}$ is an eigenvalue of E. Recall that $\mathscr{B}_E$ is a $(q-1)$-regular graph so

$$\left| q^2 - 1 - \frac{\lambda_j^2}{q^{d-2}} \right| \leq q - 1.$$

This inequality implies that $|\lambda_j| \leq q^{d/2}(1 + q^{-2})^{1/2} \leq 2q^{d/2}$. □

Proof of Theorem 9.1.8. Let $\mathscr{A}, \mathscr{B}, \mathscr{C} \subset Q$ where Q is a finite quasifield with q elements. Given $\gamma \in Q$, let

$$Z_\gamma = \{(a, b, c) \in \mathscr{A} \times \mathscr{B} \times \mathscr{C} : a + b \cdot c = \gamma\}.$$

We have $\sum_\gamma |Z_\gamma| = |\mathscr{A}||\mathscr{B}||\mathscr{C}|$ so by the Cauchy-Schwarz inequality,

$$|\mathscr{A}|^2 |\mathscr{B}|^2 |\mathscr{C}|^2 = \left(\sum_\gamma |Z_\gamma| \right)^2 \leq |\mathscr{A} + \mathscr{B} \cdot \mathscr{C}| \sum_{\gamma \in Q} |Z_\gamma|^2. \tag{9.4.6}$$

Let $x = \sum_\gamma |Z_\gamma|^2$. By (9.4.6),

$$|\mathscr{A} + \mathscr{B} \cdot \mathscr{C}| \geq \frac{|\mathscr{A}|^2 |\mathscr{B}|^2 |\mathscr{C}|^2}{x}. \tag{9.4.7}$$

The integer x is the number of ordered triples (a, b, c), (a', b', c') in $\mathscr{A} \times \mathscr{B} \times \mathscr{C}$ such that $a + b \cdot c = a' + b' \cdot c'$. This equation can be rewritten as

$$a - a' = -b \cdot c + b' \cdot c' = b \cdot (-c) + b' \cdot c'.$$

Thus, x is the number of edges between the sets

$$S = \{(a, b, b')_X : a \in \mathscr{A}, b, b' \in \mathscr{B}\}$$

and

$$T = \{(-a', -c, c')_Y : a' \in \mathscr{A}, c, c' \in \mathscr{C}\}$$

in the graph $\mathscr{SP}_Q(0)$. By Lemma 9.2.4,

$$x = e(S,T) \leq \frac{|S||T|}{q} + q^{1/2}\sqrt{|S||T|}.$$

This inequality together with (9.4.7) gives

$$\frac{|\mathscr{A}|^2|\mathscr{B}|^2|\mathscr{C}|^2}{|\mathscr{A}+\mathscr{B}\cdot\mathscr{C}|} = x \leq \frac{|\mathscr{A}|^2|\mathscr{B}|^2|\mathscr{C}|^2}{q} + q|\mathscr{A}||\mathscr{B}||\mathscr{C}|$$

from which we deduce that

$$|\mathscr{A}+\mathscr{B}\cdot\mathscr{C}| \geq q - \frac{q^3}{|\mathscr{A}||\mathscr{B}||\mathscr{C}| + q^2}$$

□

We note that as a corollary, if $|\mathscr{A}||\mathscr{B}||\mathscr{C}| > q^3 - q^2$ then $\mathscr{A}+\mathscr{B}\cdot\mathscr{C} = Q$.

Proof of Theorem 9.1.11. Let $\mathscr{A} \subset Q$, $S = -\mathscr{A} \times \mathscr{A}^d$, $T = -\mathscr{A} \times \mathscr{A}^d$, and view S as a subset of X and T as a subset of Y in the graph $\mathscr{SP}_Q(\gamma)$. By Lemmas 9.2.4 and 9.4.2,

$$\left| e(S,T) - \frac{q^d|S||T|}{q^{d+1}} \right| \leq 2q^{d/2}\sqrt{|S||T|}.$$

An edge between S and T corresponds to a solution to

$$-a_1 - a_1' + \gamma = a_2 \cdot a_2' + \cdots + a_{d+1} \cdot a_{d+1}'$$

with $a_i, a_i' \in \mathscr{A}$. If $|\mathscr{A}| \geq 2q^{\frac{d+2}{2d+2}}$, then $e(S,T) > 0$. Since γ is an arbitrary element of Q, we get

$$Q = \mathscr{A} + \mathscr{A} + \underbrace{\mathscr{A}\cdot\mathscr{A} + \cdots + \mathscr{A}\cdot\mathscr{A}}_{d \text{ terms}}$$

which completes the proof of Theorem 9.1.11. □

9.5 Proofs of Theorems 9.1.13 and 9.1.15

Let Q be a finite quasifield with q elements and let K be the kernel of Q. The *product graph*, denoted $\mathscr{DP}_Q$, is the bipartite graph with parts X and Y where X and Y are disjoint copies of Q^3. The vertex $(x_1,x_2,x_3)_X \in X$ is adjacent to $(y_1,y_2,y_3)_Y \in Y$ if and only if

$$x_3 = x_1 \cdot y_1 + x_2 \cdot y_2 + y_3. \tag{9.5.1}$$

Lemma 9.5.1. *The graph $\mathscr{DP}_Q$ is q^2-regular.*

Proof. Fix a vertex $(x_1,x_2,x_3)_X \in X$. We can choose y_1 and y_2 arbitrarily and then (9.5.1) gives a unique solution for y_3. Therefore, $(x_1,x_2,x_3)_X$ has degree q^2. A similar argument shows that every vertex in Y has degree q^2. □

Lemma 9.5.2. *If $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of $\mathscr{DP}_Q$, then $|\lambda| \leq q$ where $\lambda = \max_{i\neq 1,n} |\lambda_i|$.*

Proof. Let M be the adjacency matrix of $\mathscr{DP}_Q$. Assume that the first q^3 rows/columns of M correspond to the vertices of X. We can write

$$M = \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}$$

where N is the $q^3 \times q^3$ matrix whose $(x_1,x_2,x_3)_X \times (y_1,y_2,y_3)_Y$-entry is 1 if (9.5.1) holds and is 0 otherwise. Let J be the $q^3 \times q^3$ matrix of all 1's and let

$$P = \begin{pmatrix} 0 & J \\ J & 0 \end{pmatrix}.$$

We claim that

$$M^3 = q^2 M + q(q^2-1)P. \tag{9.5.2}$$

The (x,y)-entry of M^3 is the number of walks of length 3 from $x = (x_1,x_2,x_3)_X$ to $y = (y_1,y_2,y_3)_Y$. Suppose that $xy'x'y$ is such a walk where $y' = (y_1',y_2',y_3')_Y$ and $x' = (x_1',x_2',x_3')_X$. By Lemma 9.5.1, there are q^2 vertices $x' \in X$ such that x' is adjacent to y. In order for $xy'x'y$ to be a walk of length 3, y' must be adjacent to both x and x' so we need

$$x_3 = x_1 \cdot y_1' + x_2 \cdot y_2' + y_3' \tag{9.5.3}$$

and

$$x_3' = x_1' \cdot y_1' + x_2' \cdot y_2' + y_3'. \tag{9.5.4}$$

We want to count the number of y' that satisfy both (9.5.3) and (9.5.4). We consider two cases.

Case 1: x is not adjacent to y.

If $x_1 = x_1'$ and $x_2 = x_2'$, then (9.5.3) and (9.5.4) imply that $x_3 = x_3'$. This implies $x = x'$ and so x is adjacent to y but this contradicts our assumption that x is not adjacent to y. Therefore, $x_1 \neq x_1'$ or $x_2 \neq x_2'$. Without loss of generality, assume that $x_1 \neq x_1'$. Subtracting (9.5.4) from (9.5.3) gives

$$x_3 - x_3' + x_1' \cdot y_1' + x_2' \cdot y_2' = x_1 \cdot y_1' + x_2 \cdot y_2'. \tag{9.5.5}$$

Choose $y_2' \in Q$. Since Q is a quasifield and $x_1 - x_1' \neq 0$, there is a unique solution for y_1' in (9.5.5). Equation (9.5.3) then gives a unique solution for y_3' and so there are q choices for $y' = (y_1', y_2', y_3')_Y$ for which both (9.5.3) and (9.5.4) hold. In this case, the number of walks of length 3 from x to y is $(q^2-1)q$ since x' may be chosen in q^2-1 ways as we require $(x_1', x_2') \neq (x_1, x_2)$.

Case 2: x is adjacent to y.

The same counting as in Case 1 shows that there are $(q^2-1)q$ paths $xy'x'y$ with $x \neq x'$. By Lemma 9.5.1, there are q^2 paths of the form $xy'xy$ since the degree of x is q^2.

From the two cases, we deduce that

$$M^3 = q^2 M + q(q^2-1)P.$$

Let λ_j be an eigenvalue of M with $j \neq 1$ and $j \neq n$. Let v_j be an eigenvector for λ_j. Since v_j is orthogonal to $\chi_X + \chi_Y$ and $\chi_X - \chi_Y$, we have $Pv_j = 0$ and so

$$M^3 v_j = q^2 M v_j.$$

This gives $\lambda_j^3 = q^2 \lambda_j$ so $|\lambda_j| \leq q$. □

Proof of Theorem 9.1.13. Let $\gamma \in Q^*$ and $\mathscr{A}, \mathscr{B}, \mathscr{C}, \mathscr{D} \subset Q$. For each pair $(b,d) \in \mathscr{B} \times \mathscr{D}$, define

$$L_\gamma(b,d) = \{(b \cdot \lambda, d \cdot \lambda, -\gamma \cdot \lambda)_Y : \lambda \in K^*\}.$$

Claim 1: If $(a,c) \in \mathscr{A} \times \mathscr{C}$ and $a \cdot b + c \cdot d = \gamma$, then $(a,c,0)_X$ is adjacent to every vertex in $L_\gamma(b,d)$.

Proof. Assume $(a,c) \in \mathscr{A} \times \mathscr{C}$ satisfies $a \cdot b + c \cdot d = \gamma$. If $\lambda \in K^*$, then

$$a \cdot (b \cdot \lambda) + c \cdot (d \cdot \lambda) = (a \cdot b) \cdot \lambda + (c \cdot d) \cdot \lambda = (a \cdot b + c \cdot d) \cdot \lambda = \gamma \cdot \lambda.$$

Therefore, $0 = a \cdot (b \cdot \lambda) + c \cdot (d \cdot \lambda) - \gamma \cdot \lambda$ which shows that $(a,c,0)_X$ is adjacent to $(b \cdot \lambda, d \cdot \lambda, -\gamma \cdot \lambda)_Y$.

Claim 2: If $(b_1,d_1) \neq (b_2,d_2)$, then $L_\gamma(b_1,d_1) \cap L_\gamma(b_2,d_2) = \emptyset$.

Proof. Suppose that $L_\gamma(b_1,d_1) \cap L_\gamma(b_2,d_2) \neq \emptyset$. There are elements $\lambda, \beta \in K^*$ such that

$$(b_1 \cdot \lambda, d_1 \cdot \lambda, -\gamma \cdot \lambda)_Y = (b_2 \cdot \beta, d_2 \cdot \beta, -\gamma \cdot \beta)_Y.$$

This implies

$$b_1 \cdot \lambda = b_2 \cdot \beta, \;\; d_1 \cdot \lambda = d_2 \cdot \beta, \;\; \text{and} \;\; \gamma \cdot \lambda = \gamma \cdot \beta.$$

Since $\gamma \cdot \lambda = \gamma \cdot \beta$, we have $\gamma \cdot (\lambda - \beta) = 0$. As $\gamma \neq 0$, we must have $\lambda = \beta$ so $b_1 \cdot \lambda = b_2 \cdot \beta = b_2 \cdot \lambda$. Using Lemma 9.2.1,

$$0 = b_1 \cdot \lambda - (b_2 \cdot \lambda) = b_1 \cdot \lambda + (-b_2) \cdot \lambda = (b_1 - b_2) \cdot \lambda.$$

Since $\lambda \neq 0$, we have $b_1 = b_2$. A similar argument shows that $d_1 = d_2$.

Let $S = \{(a,c,0)_X : a \in \mathscr{A}, c \in \mathscr{C}\}$ and

$$T = \bigcup_{(b,d) \in \mathscr{B} \times \mathscr{D}} L_\gamma(b,d).$$

The number of edges between S and T in $\mathscr{D}\mathscr{P}_Q$ is $N_\gamma(|K|-1)$ where N_γ is the number of 4-tuples $(a,b,c,d) \in \mathscr{A} \times \mathscr{B} \times \mathscr{C} \times \mathscr{D}$ such that $a \cdot b + c \cdot d = \gamma$. Furthermore $|S| = |\mathscr{A}||\mathscr{C}|$ and $|T| = |\mathscr{B}||\mathscr{D}|(|K|-1)$ by Claim 2. By Lemmas 9.2.4 and 9.5.2,

$$\left| N_\gamma(|K|-1) - \frac{|S||T|}{q} \right| \leq q\sqrt{|S||T|}. \tag{9.5.6}$$

This equation is equivalent to

$$\left| N_\gamma - \frac{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{q} \right| \leq q \left(\frac{|\mathscr{A}||\mathscr{B}||\mathscr{C}||\mathscr{D}|}{|K|-1} \right)^{1/2}$$

which completes the proof of Theorem 9.1.13. □

The proof of Theorem 9.1.15 is similar to the proof of Theorem 9.1.13. Instead of working with the graph $\mathscr{DP}_Q$, one works with the graph $\mathscr{DP}_{Q,d}$ which we define to be the bipartite graph with parts X and Y where these sets are disjoint copies of Q^{d+1}. The vertex $(x_1,\ldots,x_{d+1})_X \in X$ is adjacent to $(y_1,\ldots,y_{d+1})_Y \in Y$ if and only if

$$x_{d+1} = x_1 \cdot y_1 + \cdots + x_d \cdot y_d + y_{d+1}.$$

It is easy to show that $\mathscr{DP}_{q,d}$ is q^d-regular. Equation (9.5.2) will become

$$M^3 = q^d M + q^{d-1}(q^d - 1)P$$

which will lead to the bound of $\lambda \leq q^{d/2}$ where $\lambda = \max_{i\neq 1,n} |\lambda_i|$ and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of $\mathscr{DP}_{q,d}$. One then counts edges between the sets

$$S = \{(a'_1,\ldots,a'_d,0)_X : a'_i \in \mathscr{A}\}$$

and

$$T = \bigcup_{(a_1,\ldots,a_d)\in\mathscr{A}^d} L_\gamma(a_1,\ldots,a_d)$$

where $L_\gamma(a_1,\ldots,a_d) = \{(a_1\cdot\lambda,\ldots,a_d\cdot\lambda,-\gamma\cdot\lambda)_Y : \lambda \in K^*\}$. The remaining details are left to the reader.

10 Open problems

In this chapter, we mention some open problems on Erdős distinct distances problem and related problems.

10.1 Erdős distinct distances problem in $\mathbb{F}_q^d$

On the Erdős distinct distances problem in $\mathbb{F}_q^d$ with d even, the following conjecture was made by Iosevich [43].

Conjecture 10.1.1 (**Iosevich**, [43])**.** *Let $\mathcal{E}$ be a set in $\mathbb{F}_q^d$ with d even. Suppose that $|\mathcal{E}| \gg q^{\frac{d}{2}+\frac{1}{3}}$, then $\mathcal{E}$ determines a positive proportion of all distances.*

We note that in the case $d = 2$, this conjecture was proved by Bennett, Hart, Iosevich, Pakianathan and Rudnev [6] in 2013 by using Fourier analytic methods. In 2015, Hanson, Lund, Roche-Newton [32] reproved this result by using geometric properties of rotations and reflections in the plane $\mathbb{F}_q^2$.

It has been mentioned in Chapter 4 that for a set $\mathcal{E} \subseteq S_1$, if $|\mathcal{E}| \gg q^{\frac{d}{2}}$, then the distance set contains a positive proportion of all distances. However, there is no known result for the case when $\mathcal{E}$ is a set on a paraboloid defined as follows:

$$P := \left\{\mathbf{x} \in \mathbb{F}_q^d \colon x_1^2 + \cdots + x_{d-1}^2 = x_d\right\}.$$

Thus we are led to the following question:

Question 10.1.2. *Is it true that for a subset $\mathcal{E}$ on a paraboloid in $\mathbb{F}_q^d$, $d \geq 3$, if $|\mathcal{E}| \gg q^{d/2}$, then $|\Delta_{\mathbb{F}_q}(\mathcal{E})| \gg q$?*

10.2 Distribution of simplices

In d-dimensional vector space $\mathbb{F}_q^d$, two k-simplices with vertices $(\mathbf{x}_1,\dots,\mathbf{x}_{k+1})$ and $(\mathbf{y}_1,\dots,\mathbf{y}_{k+1})$ are called to be in the same congruence class if there exist an orthogonal matrix $\theta \in O(d,\mathbb{F}_q)$ and an element $\mathbf{z} \in \mathbb{F}_q^d$ so that $\mathbf{z}+\theta(\mathbf{x}_i)=\mathbf{y}_i$ for all $i=1,2,\dots,k+1$, where $O(d,\mathbb{F}_q)$ is the orthogonal group in $\mathbb{F}_q^d$. For $\mathscr{E} \subseteq \mathbb{F}_q^d$ and $1 \le k \le d$, let $T_{k,d}(\mathscr{E})$ be the number of congruence classes of k-simplices generated by $\mathscr{E}$. In the spirit of the distance results, Hart and Iosevich [34] studied the following question:

Question 10.2.1. *For $\mathscr{E} \subseteq \mathbb{F}_q^d$, how large does $\mathscr{E}$ need to be to guarantee that $T_{k,d}(\mathscr{E}) \gg q^{\binom{k+1}{2}}$?*

Hart and Iosevich [34] proved that when $|\mathscr{E}| \gg q^{\frac{kd}{k+1}+\frac{k}{2}}$ and $d \ge \binom{k+1}{2}$, we have $T_{k,d}(\mathscr{E}) \gg q^{\binom{k+1}{2}}$. There were several progresses on improving this result in recent years, for example, see [12, 86]. The best known result was established by Bennett, Hart, Iosevich, Pakianathan, and Rudnev [6] by using Fourier analytic methods and results from group action theory. Precisely, they proved that for $1 \le k \le d$ and $|\mathscr{E}| \gg q^{d-\frac{d-1}{k+1}}$, we have $T_{k,d}(\mathscr{E}) \gg q^{\binom{k+1}{2}}$. The authors of [6] also gave a construction of a set $\mathscr{E} = \mathbb{F}_q^{d-1} \times \mathscr{A} \subseteq \mathbb{F}_q^d$ with $|\mathscr{E}| = q^{d-1+\frac{1}{d}-\varepsilon}$ for some $\varepsilon > 0$ and $T_{d,d}(\mathscr{E}) = o\left(q^{\binom{d+1}{2}}\right)$. It follows from this construction that when $k < d$, we always can find a set $\mathscr{E}$ in a k-dimensional subspace with $|\mathscr{E}| = q^{k-1+\frac{1}{k}-\varepsilon}$ for some $\varepsilon > 0$ and $T_{k,d}(\mathscr{E}) = o\left(q^{\binom{k+1}{2}}\right)$. In other words, if we assume that $\alpha_{k,d}$ is the infimum of numbers $t > 0$ such that when $|\mathscr{E}| \gg q^t$ the number of congruence classes of k-simplices in $\mathscr{E}$ is $cq^{\binom{k+1}{2}}$ for some positive constant c, then we have $\alpha_{k,d} \ge k-1+\frac{1}{k}$.

In the case $d=k=2$, Bennett, Hart, Iosevich, Pakianathan and Rudnev [6] proved that for $\mathscr{E} \subseteq \mathbb{F}_q^2$, if $|\mathscr{E}| \gg q^{8/5}$, then $\mathscr{E}$ generates a positive proportion of all congruence classes of triangles. From this result and the construction on k-simplices in [6], Iosevich [43] conjectured the following.

Conjecture 10.2.2 (**Iosevich**, [43])**.** *Let $\mathscr{E}$ be a set in $\mathbb{F}_q^2$. Suppose that $|\mathscr{E}| \gg q^{3/2}$, then $\mathscr{E}$ determines a positive proportion of all congruence classes of triangles.*

We conclude this section with some ideas to attack the Conjecture 10.2.2 which come form the arguments in [6]. For a fixed orthogonal matrix θ, the function $w_\theta(\mathbf{z})$ in $\mathbf{z} \in \mathbb{F}_q^2$ is defined as $w_\theta(\mathbf{z}) := \#\left\{(\mathbf{u},\mathbf{v}) \in \mathscr{E}^2 : \theta\cdot\mathbf{u}+\mathbf{z}=\mathbf{v}\right\}$. Let N be the number of pairs of congruent triangles in $\mathscr{E}$. Then by the Cauchy-Schwarz inequality, we have that $T_{2,2}(\mathscr{E}) \ge |\mathscr{E}|^6/N$. On the other hand, one can check that $N \ll \sum_{\theta,\mathbf{z}} w_\theta(\mathbf{x})^3$. It has been

shown in [6] that

$$\sum_{\theta,\mathbf{z}} w_\theta(\mathbf{x})^3 \ll \frac{|\mathscr{E}|^6}{q^3} + \sum_{\theta,\mathbf{z}} ||w_\theta(\mathbf{z})||_\infty \left(w_\theta(\mathbf{z}) - \frac{|\mathscr{E}|^2}{q^2} \right)^2.$$

In [6], the authors used a trivial upper bound of $||w_\theta(\mathbf{z})||_\infty$, i.e. $||w_\theta(\mathbf{z})||_\infty \leq |\mathscr{E}|$, to give an upper bound for $\sum_{\theta,\mathbf{z}} w_\theta(\mathbf{x})^3$. Thus we can expect to improve the exponent 8/5 by considering $||w_\theta(\mathbf{z})||_\infty$ carefully. The following question was raised by Gábor Tardos:

Question 10.2.3. *Is this true that for almost all of orthogonal matrices θ, there exists a threshold $t = o(|\mathscr{E}|)$ such that the following holds*

$$\sum_{\mathbf{z}\in\mathbb{F}_q^2, ||w_\theta(\mathbf{z})||_\infty < t} t \cdot w_\theta(\mathbf{z})^2 > \frac{1}{2} \sum_{\mathbf{z}\in\mathbb{F}_q^2} ||w_\theta(\mathbf{z})||_\infty w_\theta(\mathbf{z})^2 \, ?$$

10.3 Schwartz-Zippel lemma and generalizations

A special case of the well-known Schwartz-Zippel lemma states that for an algebraic curve $\mathscr{C} \subset \mathbb{C}^2$ of degree d and two finite sets $\mathscr{A}, \mathscr{B} \subset \mathbb{C}$, we have the cardinality of $\mathscr{C} \cap (\mathscr{A} \times \mathscr{B})$ is at most $O_d(|\mathscr{A}| + |\mathscr{B}|)$. In other words, it bounds the size of the intersection of an algebraic curve with a Cartesian product of *one-dimensional* sets. In [55], we proved two generalizations of this result for varieties in $\mathbb{C}^4$. More precisely, given a variety $X \subset \mathbb{C}^4$ and two finite sets $\mathscr{E}, \mathscr{F} \subset \mathbb{C}^2$, we gave upper bounds on the size of the intersection $X \cap (\mathscr{E} \times \mathscr{F})$, and we determine which X can contain a whole product $\mathscr{E} \times \mathscr{F}$. Note that we can not expect a good bound on $|X \cap (\mathscr{E} \times \mathscr{F})|$ for all varieties. For example, let $X = Z(P)$ where $P = G(x,y)H(x,y,s,t) + K(s,t)L(x,y,s,t)$, with $H, L \in \mathbb{C}[x,y,s,t]$ and $G \in \mathbb{C}[x,y]\backslash\mathbb{C}$ and $K \in \mathbb{C}[s,t]\backslash\mathbb{C}$, if $\mathscr{E} \subset Z(G)$ and $\mathscr{F} \subset Z(K)$, then X contains $\mathscr{E} \times \mathscr{F}$. From this example, we are led to the following definition.

Let X be a variety in $\mathbb{C}^4$ and $I(X)$ be its ideal in $\mathbb{C}[x,y,s,t]$. We say that X is *Cartesian* if there exist $G \in \mathbb{C}[x,y]\backslash\mathbb{C}$ and $K \in \mathbb{C}[s,t]\backslash\mathbb{C}$ such that for any $P \in I(X)$, P can be written as

$$P(x,y,s,t) = G(x,y)H(x,y,s,t) + K(s,t)L(x,y,s,t),$$

where $H(x,y,s,t), L(x,y,s,t) \in \mathbb{C}[x,y,s,t]$. Our first main result in [55] is for the case of one or two dimensional non-Cartesian varieties in $\mathbb{C}^4$.

Theorem 10.3.1 (**Mojarrad-Pham-Valculescu-de Zeeuw**, [55])**.** *Let X be a non-Cartesian variety in $\mathbb{C}^4$ of degree d and dimension one or two, and $\mathscr{E}, \mathscr{F}$ be finite sets in $\mathbb{C}^2$. We have the cardinality of $X \cap (\mathscr{E} \times \mathscr{F})$ is at most $O_d(|\mathscr{E}| + |\mathscr{F}|)$.*

Our second main result in [55] is for the case of three dimensional non-Cartesian

varieties in $\mathbb{C}^4$.

Theorem 10.3.2 (**Mojarrad-Pham-Valculescu-de Zeeuw**, [55])**.** *Let X be a non-Cartesian variety of degree d and dimension three in $\mathbb{C}^4$, and $\mathscr{E},\mathscr{F}$ be finite sets in $\mathbb{C}^2$. We have the cardinality of $X \cap (\mathscr{E} \times \mathscr{F})$ is at most $O_{d,\varepsilon}\left(|\mathscr{E}|^{2/3+\varepsilon}|\mathscr{F}|^{2/3} + |\mathscr{E}| + |\mathscr{F}|\right)$. Note that if $\mathscr{E},\mathscr{F} \subset \mathbb{R}^2$, the ε can be omitted.*

We note here that the Szemerédi-Trotter theorem [77], which bounds the number of incidences between points and lines in $\mathbb{R}^2$, can be rephrased as the case $F = xs - y + t$ of Theorem 10.3.2. We refer the reader to [55] for more discussions and for sharpness of Theorems 10.3.1 and 10.3.2.

We conclude this chapter with the following problem:

Problem 10.3.3. *Give generalizations of Theorem 10.3.2 in the setting of arbitrary fields.*

Bibliography

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev, and I. Shkredov, *Growth estimates in positive characteristic via collisions*, International Mathematics Research Notices, (2015).

[2] E. Bannai, O. Shimabukuro, and H. Tanaka, *Finite analogues of non-euclidean spaces and ramanujan graphs*, European Journal of Combinatorics, 25 (2004), pp. 243–259.

[3] B. Barak, R. Impagliazzo, and A. Wigderson, *Extracting randomness using few independent sources*, SIAM Journal on Computing, 36 (2006), pp. 1095–1118.

[4] M. Benett, *Right angles in* $\mathbb{F}_q^d$, arXiv:1511.08942, (2015).

[5] M. Bennett, J. Chapman, D. Covert, D. Hart, A. Iosevich, and J. Pakianathan, *Long paths in the distance graph over large subsets of vector spaces over finite fields*, J. Korean Math. Soc, 53 (2016), pp. 115–126.

[6] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, and M. Rudnev, *Group actions and geometric combinatorics in* $\mathbb{F}_q^d$, Forum Mathematicum, (2016).

[7] M. Bennett, A. Iosevich, and J. Pakianathan, *Three-point configurations determined by subsets of* $\mathbb{F}_q^2$ *via the elekes-sharir paradigm*, Combinatorica, 34 (2014), pp. 689–706.

[8] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, International Journal of Number Theory, 1 (2005), pp. 1–32.

[9] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geometric & Functional Analysis GAFA, 14 (2004), pp. 27–57.

[10] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-transitive graphs*, in Distance-Regular Graphs, Springer, 1989, pp. 214–234.

[11] B. BUKH AND J. TSIMERMAN, *Sum–product estimates for rational functions*, Proceedings of the London Mathematical Society, (2011), p. pdr018.

[12] J. CHAPMAN, M. B. ERDOGAN, D. HART, A. IOSEVICH, AND D. KOH, *Pinned distance sets, k-simplices, wolff's exponent in finite fields and sum-product estimates*, Mathematische Zeitschrift, 271 (2012), pp. 63–93.

[13] M. CHARALAMBIDES, *A note on distinct distance subsets*, Journal of Geometry, 104 (2013), pp. 439–442.

[14] J. CILLERUELO, *Combinatorial problems in finite fields and sidon sets*, Combinatorica, 32 (2012), pp. 497–511.

[15] J. CILLERUELO, A. IOSEVICH, B. LUND, O. ROCHE-NEWTON, AND M. RUDNEV, *Elementary methods for incidence problems in finite fields*, To appear in Actar Arithmetica, (2016).

[16] D. CONLON, J. FOX, W. GASARCH, D. G. HARRIS, D. ULRICH, AND S. ZBARSKY, *Distinct volume subsets*, SIAM Journal on Discrete Mathematics, 29 (2015), pp. 472–480.

[17] D. COVERT, D. HART, A. IOSEVICH, D. KOH, AND M. RUDNEV, *Generalized incidence theorems, homogeneous forms and sum–product estimates in finite fields*, European Journal of Combinatorics, 31 (2010), pp. 306–319.

[18] D. COVERT, A. IOSEVICH, AND J. PAKIANATHAN, *Geometric configurations in the ring of integers modulo p^l*, Indiana university mathematics journal, 61 (2012), pp. 1949–1969.

[19] D. COVERT, D. KOH, AND Y. PI, *The k-resultant modulus set problem on algebraic varieties over finite fields*, arXiv preprint arXiv:1508.02688, (2015).

[20] F. DE ZEEUW, *A short proof of rudnev's point-plane incidence bound*, arXiv preprint arXiv:1612.02719, (2016).

[21] P. DEMBOWSKI, *Finite Geometries: Reprint of the 1968 edition*, Springer Science & Business Media, 2012.

[22] G. ELEKES, *On the number of sums and products*, Acta Arithmetica, 81 (1997), pp. 365–367.

[23] G. ELEKES, M. B. NATHANSON, AND I. Z. RUZSA, *Convexity and sumsets*, Journal of Number Theory, 83 (2000), pp. 194–201.

[24] G. ELEKES AND L. RÓNYAI, *A combinatorial problem on polynomials and rational functions*, Journal of Combinatorial Theory, Series A, 89 (2000), pp. 1–20.

[25] P. ERDŐS, *On sets of distances of n points*, The American Mathematical Monthly, 53 (1946), pp. 248–250.

[26] P. ERDŐS AND E. SZEMERÉDI, *On sums and products of integers*, Studies in Pure Mathematics, Basel; Birkhäuser, (1983), pp. 213–218.

[27] M. GARAEV, *The sum-product estimate for large subsets of prime fields*, Proceedings of the American Mathematical Society, 136 (2008), pp. 2735–2739.

[28] N. GILL, H. HELFGOTT, AND M. RUDNEV, *On growth in an abstract plane*, Proceedings of the American Mathematical Society, 143 (2015), pp. 3593–3602.

[29] L. GUTH AND N. H. KATZ, *On the erdős distinct distances problem in the plane*, Annals of Mathematics, 181 (2015), pp. 155–190.

[30] K. GYARMATI AND A. SÁRKÖZY, *Equations in finite fields with restricted solution sets. ii (algebraic equations)*, Acta Mathematica Hungarica, 119 (2008), pp. 259–280.

[31] L. Q. HAM, P. THANG, AND L. A. VINH, *Conditional expanding bounds for two-variable functions over finite valuation rings*, European Journal of Combinatorics, 60 (2017), pp. 114–123.

[32] B. HANSON, B. LUND, AND O. ROCHE-NEWTON, *On distinct perpendicular bisectors and pinned distances in finite fields*, Finite Fields and Their Applications, 37 (2016), pp. 240–264.

[33] D. HART AND A. IOSEVICH, *Sums and products in finite fields: an integral geometric viewpoint*, Radon transforms, geometry, and wavelets, 464 (2008), pp. 129–135.

[34] ——, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Analysis Mathematica, 34 (2008), pp. 29–38.

[35] D. HART, A. IOSEVICH, D. KOH, AND M. RUDNEV, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the erdős-falconer distance conjecture*, Transactions of the American Mathematical Society, 363 (2011), pp. 3255–3275.

[36] D. HART, A. IOSEVICH, AND J. SOLYMOSI, *Sum-product estimates in finite fields via kloosterman sums*, IMRN-International Mathematics Research Notices, 2007 (2007), p. rnm007.

[37] D. HART, L. LI, AND C.-Y. SHEN, *Fourier analysis and expanding phenomena in finite fields*, Proceedings of the American Mathematical Society, 141 (2013), pp. 461–473.

[38] N. HEGYVÁRI AND F. HENNECART, *Explicit constructions of extractors and expanders*, Acta Arithmetica, 140 (2009), p. 233.

[39] ——, *Conditional expanding bounds for two-variable functions over prime fields*, European Journal of Combinatorics, 34 (2013), pp. 1365–1382.

[40] H. A. HELFGOTT AND M. RUDNEV, *An explicit incidence theorem in* $\mathbb{F}_p$, Mathematika, 57 (2011), pp. 135–145.

[41] D. D. HIEU AND L. A. VINH, *On distance sets and product sets in vector spaces over finite rings*, Michigan Math. J, 62 (2013), pp. 000–000.

[42] D. R. HUGHES AND F. C. PIPER, *Projective planes*, vol. 6, Springer, 1973.

[43] A. IOSEVICH, *The first vietnam workshop on graph theory and discrete mathematics*, Hanoi, (2016).

[44] A. IOSEVICH AND M. RUDNEV, *Erdős distance problem in vector spaces over finite fields*, Transactions of the American Mathematical Society, 359 (2007), pp. 6127–6142.

[45] D. KOH AND C.-Y. SHEN, *The generalized erdős–falconer distance problems in vector spaces over finite fields*, Journal of Number Theory, 132 (2012), pp. 2455–2473.

[46] D. KOH AND H.-S. SUN, *Distance sets of two subsets of vector spaces over finite fields*, Proceedings of the American Mathematical Society, 143 (2015), pp. 1679–1692.

[47] S. V. KONYAGIN AND M. RUDNEV, *On new sum-product–type estimates*, SIAM Journal on Discrete Mathematics, 27 (2013), pp. 973–990.

[48] S. V. KONYAGIN AND I. D. SHKREDOV, *On sum sets of sets having small product set*, Proceedings of the Steklov Institute of Mathematics, 290 (2015), pp. 288–299.

[49] M. KRIVELEVICH AND B. SUDAKOV, *Pseudo-random graphs*, More sets, graphs and numbers, (2006), pp. 199–262.

[50] W. M. KWOK, *Character tables of association schemes of affine type*, European journal of combinatorics, 13 (1992), pp. 167–185.

[51] H. LEFMANN AND T. THIELE, *Point sets with distinct distances*, Combinatorica, 15 (1995), pp. 379–408.

[52] L. LI AND O. ROCHE-NEWTON, *Convexity and a sum-product type estimate*, Acta Arithmetica, 156 (2012), pp. 247–255.

[53] B. LUND AND S. SARAF, *Incidence bounds for block designs*, SIAM Journal on Discrete Mathematics, 30 (2016), pp. 1997–2010.

[54] G. MOCKENHAUPT, T. TAO, ET AL., *Restriction and kakeya phenomena for finite fields*, Duke Mathematical Journal, 121 (2004), pp. 35–74.

[55] H. N. MOJARRAD, T. PHAM, C. VALCULESCU, AND F. DE ZEEUW, *Schwartz-zippel bounds for two-dimensional products*, arXiv preprint arXiv:1507.08181, (2015).

[56] B. MURPHY, G. PETRIDIS, O. ROCHE-NEWTON, M. RUDNEV, AND I. D. SHKREDOV, *New results on sum-product type growth over fields*, arXiv preprint arXiv:1702.01003, (2017).

[57] H. H. NGUYEN, *On two-point configurations in a random set*, Integers, 9 (2009), pp. 41–45.

[58] J. PACH AND P. K. AGARWAL, *Combinatorial geometry*, vol. 37, John Wiley & Sons, 2011.

[59] J. PACH AND G. TARDOS, *Isosceles triangles determined by a planar point set*, Graphs and Combinatorics, 18 (2002), pp. 769–779.

[60] G. PETRIDIS, *Pinned algebraic distances determined by cartesian products in* $\mathbb{F}_p^2$, arXiv:1610.03172, (2016).

[61] T. PHAM, L. A. VINH, AND F. DE ZEEUW, *Three-variable expanding polynomials and higher-dimensional distinct distances*, arXiv preprint arXiv:1612.09032, (2016).

[62] O. E. RAZ, M. SHARIR, AND F. DE ZEEUW, *The elekes-szabó theorem in four dimensions*, arXiv:1607.03600, (2016).

[63] O. E. RAZ, M. SHARIR, AND J. SOLYMOSI, *Polynomials vanishing on grids: The elekes–rónyai problem revisited*, American Journal of Mathematics, 138 (2016), pp. 1029–1065.

[64] O. ROCHE-NEWTON, M. RUDNEV, AND I. D. SHKREDOV, *New sum-product type estimates over finite fields*, Advances in Mathematics, 293 (2016), pp. 589–605.

[65] M. RUDNEV, *An improved sum–product inequality in fields of prime order.*, IMRN: International Mathematics Research Notices, 2012 (2012).

[66] ——, *On the number of incidences between planes and points in three dimensions*, Combinatorica, (2014).

[67] A. SÁRKÖZY, *On sums and products of residues modulo p*, Acta Arithmetica, 118 (2005), pp. 403–409.

[68] ——, *On products and shifted products of residues modulo p*, Integers, 8 (2008).

[69] R. SCHWARTZ, J. SOLYMOSI, AND F. DE ZEEUW, *Extensions of a result of elekes and rónyai*, Journal of Combinatorial Theory, Series A, 120 (2013), pp. 1695–1713.

[70] A. SHEFFER, *Distinct distances: open problems and current bounds*, arXiv:1406.1949, (2014).

[71] I. E. SHPARLINSKI, *On the additive energy of the distance set in finite fields*, Finite Fields and Their Applications, 42 (2016), pp. 187–199.

[72] J. SOLYMOSI, *Bounding multiplicative energy by the sumset*, Advances in mathematics, 222 (2009), pp. 402–408.

[73] J. SOLYMOSI, *Incidences and the spectra of graphs*, in Combinatorial Number Theory and Additive Group Theory, Springer, 2009, pp. 299–314.

[74] J. SOLYMOSI AND V. H. VU, *Near optimal bounds for the erdős distinct distances problem in high dimensions*, Combinatorica, 28 (2008), pp. 113–125.

[75] J. SPENCER, *Turán's theorem for k-graphs*, Discrete Mathematics, 2 (1972), pp. 183–186.

[76] S. STEVENS AND F. DE ZEEUW, *An improved point-line incidence bound over arbitrary fields*, arXiv:1609.06284, (2016).

[77] E. SZEMERÉDI AND W. T. TROTTER JR, *Extremal problems in discrete geometry*, Combinatorica, 3 (1983), pp. 381–392.

[78] TAO, *Additive Combinatorics (Cambridge studies in advanced mathematics; 105)*, Cambridge University Press, 2006.

[79] T. TAO, *The sum-product phenomenon in arbitrary rings*, Contributions to Discrete Mathematics, 4 (2009).

[80] ——, *Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets*, Contributions to Discrete Mathematics, 10 (2015).

[81] A. TERRAS, *Survey of spectra of laplacians on finite symmetric spaces*, Experimental Mathematics, 5 (1996), pp. 15–32.

[82] P. V. THANG AND L. A. VINH, *Erdős–rényi graph, szemerédi–trotter type theorem, and sum-product estimates over finite rings*, Forum Mathematicum, 27 (2015), pp. 331–342.

[83] L. A. VINH, *On a furstenberg-katznelson-weiss type theorem over finite fields*, Annals of Combinatorics, 15 (2011), pp. 541–547.

[84] ——, *On the solvability of systems of sum–product equations in finite fields*, Glasgow Mathematical Journal, 53 (2011), pp. 427–435.

[85] ——, *A szemerédi-trotter type theorem and sum-product estimate over finite fields*, Eur. J. Comb., 32 (2011), pp. 1177–1181.

[86] ——, *On kaleidoscopic pseudo-randomness of finite euclidean graphs.*, Discussiones Mathematicae: Graph Theory, 32 (2012).

[87] ——, *Graphs generated by sidon sets and algebraic equations over finite fields*, Journal of Combinatorial Theory Series B, 103 (2013), pp. 651–657.

[88] ——, *The number of occurrences of a fixed spread among n directions in vector spaces over finite fields*, Graphs and Combinatorics, 29 (2013), pp. 1943–1949.

[89] ——, *On four-variable expanders in finite fields*, SIAM Journal on Discrete Mathematics, 27 (2013), pp. 2038–2048.

[90] ——, *On the generalized erdős–falconer distance problems over finite fields*, Journal of Number Theory, 133 (2013), pp. 2939–2947.

[91] ——, *On point-line incidences in vector spaces over finite fields*, Discrete applied mathematics, 177 (2014), pp. 146–151.

[92] ——, *On three-variable expanders over finite fields*, International Journal of Number Theory, 10 (2014), pp. 689–703.

[93] ——, *The sovability of norm, bilinear and quadratic equations over finite fields via spectra of graphs*, Forum Mathematicum, 26 (2014), pp. 141–175.

[94] ——, *Product graphs, sum-product graphs and sum-product estimates over finite rings*, Forum Mathematicum, 27 (2015), pp. 1639–1655.

[95] V. H. VU, *Sum-product estimates via directed expanders*, Mathematical research letters, 15 (2008), pp. 375–388.

[96] D. ZHELEZOV, *On additive shifts of multiplicative almost-subgroups in finite fields*, to appear in Proceedings of the American Mathematical Society, (2017).

Thang Pham — Curriculum Vitae

Ecole Polytechnique Federale de Lausanne
EPFL-SB-MATHGEOM-DCG, Station 8
CH-1015 Lausanne, SWITZERLAND
thang.pham@epfl.ch
ORCID iD: 0000-0002-8514-0808
http://dcg.epfl.ch/thang

Home Address:
Ha Noi, Vietnam

Research Interests

Geometric Combinatorics and Combinatorial Number Theory

Education

1. **Ecole Polytechnique Federale de Lausanne (EPFL)**

   Ph.D., Mathematics, 01.11.2013–12.06.2017

   Advisor: János Pach

2. **University of Science, Vietnam National University, Ha Noi**

   B.Sc. in Mathematics, 2008-2012.

Employment

1. **University of California San Diego.**
   Postdoctoral Fellow: 09.2017-03.2019.
   Advisor: Andrew H Suk
2. **Chair of Combinatorial Geometry, Basis Sciences school, EPFL.**
   Assistant doctorant, 11.2013–12.06.2017.
   Advisor: János Pach
3. **Department of Algebra, Geometry and Topology, University of Science, Vietnam National University, Hanoi.**
   Lecturer, 09. 2012–09. 2013

Research Visits

Renyi Institute, 18-24, July 2016. Advisor: Gábor Tardos

Advising

Nicolas Rameier, Co-supervising bachelor project at EPFL, Fall 2015.

Nicolas Rameier, supervising master project at EPFL, Spring 2017.

Teaching Experience

TA **EPFL** Fall 2016: Geometry (Instructor: Prof. Philippe Michel)

TA **EPFL** Spring 2016: Geometry (Instructor: Prof. Peter Buser)

TA **EPFL** Fall 2015: Discrete Mathematics (Instructor: Prof. János Pach)

TA **EPFL** Spring 2015: Geometry (Instructor: Prof. Peter Buser)

TA **EPFL** Fall 2014: Linear Algebra (Instructor: Prof. János Pach)

TA **VNU** Spring 2013: Abstract algebra (Instructor: Dr. Pham Viet Hung)

TA **VNU** Fall 2012: Linear Algebra (Instructor: Prof. Pham Duc Dat)

Service

Referee for: Discrete and Computational Geometry (DCG) and SIAM Journal on Discrete Mathematics (SIDMA).

Awards

Prime Speciale at EPFL, 2016.

Excellent Project Awards in 2013 on National Program for the Development of Mathematics until 2020, (with Le Anh Vinh).

The Honda Young Engineer and Scientist Award, Honda Foundation and The National Institute for Science and Technology, 2012

Valedictorian Ha Noi Capital , Viet Nam 2012.

Prize for the best student in mathematics, University of Science, VNU, 2012.

First-rank Graduate in Department of Mathematics-Mechanics-Informatics, HUS, VNU, 2012.

Co-authors:

I have had the pleasure to work with:

Tanbir Ahmed, Arie Bialostocki, Ben Lund, Le Quang Ham, Do Duy Hieu, Pham Duc Hiep, Alex Iosevich, Doowon Koh, Hossein N. Mojarrad, Nguyen Duy Phuong, Nguyen Minh Sang, Michael Tait, Craig Timmons, Gábor Tardos, Le Anh Vinh, Claudiu Valculescu, Robert Won, Frank de Zeeuw.

My Erdős number is 2.

Workshops and conferences

The First Vietnam Workshop on Graph Theory and Discrete Geometry, Hanoi, Vietnam, September 2016

A New Era of Discrete & Computational Geometry Ascona, Switzerland, June 2016

14 th Gremo's Workshop on Open Problems, Switzerland, May 2016

Seminar on Matroids in Algebra, Representation theory and Topology, Les Diablerets, January, 2016

Ascension of Combinatorics Conference, EPFL, May 2015

25 th British Combinatorial Conference, University of Warwick, June 2015

Two-Day Workshop on Combinatorics, EPFL, February 2014

Borel Seminar 2014 at Les Diablerets, July 2014

Publications

1. **A Szemerédi-Trotter type theorem, sum-product estimates in finite quasifields, and related results**, with M. Tait, C. Timmons, L. A. Vinh, Journal of Combinatorial Theory Series A, **147** (**2017**), 55–74.
2. **Conditional expanding bounds for two-variable functions over finite valuation rings**, with L. Q. Ham, L. A. Vinh, European Journal of Combinatorics, **60** (**2017**), 114–123.
3. **Incidences between points and generalized spheres over finite fields and related problems**, with N. D. Phuong, L. A. Vinh, Forum Mathematicum, Volume **29**, Issue 2 (Mar 2017).
4. **Incidences between planes over finite fields**, with N. D. Phuong, L. A. Vinh, to appear in Proceedings of the American Mathematical Society, (2017).
5. **Distinct distances on regular varieties**, with D. D. Hieu, Journal of Number Theory, **173** (**2017**), 602–613.

6. **An improvement on the number of simplices in $\mathbb{F}_q^d$**, with P. D. Hiep, L. A. Vinh, Discrete Applied Mathematics, **221** (2017) 95–105.
7. **An additive problem in finite cyclic rings with powers of elements of large multiplicative order**, with N. M. Sang, L. A. Vinh, Applicable Analysis and Discrete Mathematics, **10** (**2016**), 325–331.
8. **Orthogonal systems in vector spaces over finite rings**, with L. A. Vinh, Electronic Journal of Combinatorics, **20**(2) (**2012**), P48.
9. **Erdős-Rényi graph, Szemerédi-Trotter type theorem, and sum-product estimates over finite rings**, with L. A. Vinh, Forum Mathematicum, Vol. 27. No. 1. **2015**.
10. **Schwartz-Zippel bounds for two-dimensional products**, with H. N. Mojarrad, C. Valculescu, F. de Zeeuw, submitted for publication, (**2016**).
11. **Distinct distances between points and lines in $\mathbb{F}_q^2$**, with N. D. Phuong, N. M. Sang, C. Valculescu, L. A. Vinh, submitted for publication, (**2016**).
12. **Some combinatorial number theory problems in finite spaces**, with L. A. Vinh, submitted for publication, (**2016**).
13. **Sumsets of the distance sets in $\mathbb{F}_q^d$**, submitted for publication, (**2017**).
14. **Paths in pseudorandom graphs and applications**, with L. A. Vinh, submitted for publication, (**2017**).
15. **Distinct spreads in vector spaces over finite fields**, with B. Lund, L. A. Vinh, submitted for publication, (**2016**).
16. **Power sum polynomials as weak and relaxed EGZ polynomials**, with T. Ahmed, A. Bialostocki, L. A. Vinh, submitted for publication, (**2017**).
17. **Three-variable expanding polynomials and higher-dimensional distinct distances**, with L. A. Vinh, F. de Zeeuw, submitted for publication, (**2017**).
18. **Right angles in finite spaces**, with N. M. Sang, G. Tardos, submitted for publication, (**2017**).
19. **Conditional expanding bounds for two-variable functions over arbitrary fields**, with H. N. Mojarrad, submitted for publication (**2017**).
20. **A structure theorem for product sets in extra special groups,** with M. Tait, L. A. Vinh, R. Won, submitted for publication (**2017**).
21. **Sum and product of distance sets over finite fields**, with A. Iosevich, D. Koh, submitted for publication, (**2017**).
22. **Expanders and applications over prime fields**, with D. Koh, H. N. Mojarrad, C. Valculescu, submitted for publication, (**2017**).

Reference

Prof. Jürgpeter Buser (Teaching)
Department of Mathematics
Ecole Polytechnique Federale de Lausanne
peter.buser@epfl.ch

Prof. A. Iosevich
Department of Mathematics
University of Rochester
iosevich@math.rochester.edu

Prof. János Pach
Chair of Combinatorial Geometry
Ecole Polytechnique Federale de Lausanne
janos.pach@epfl.ch

Prof. Le Anh Vinh
University of Education
Vietnam National University, Ha Noi
vinhla@vnu.edu.vn

Prof. Gábor Tardos
Rényi Institute, Budapest
tardos@renyi.hu